ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
Σχολή Θετικών Επιστημών
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Ασφάλεια και Προστασία της Ιδιωτικότητας σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης

Διατριβή

για την απόκτηση Διδακτορικού Διπλώματος

του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Προκόπιος Κ. Δρογκάρης

ΣΑΜΟΣ 2013

ΤΡΙΜΕΛΗΣ ΣΥΜΒΟΥΛΕΥΤΙΚΗ ΕΠΙΤΡΟΠΗ
ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ

Καθηγητής Γκρίτζαλης Στέφανος. Επιβλέπων

Τμήμα Μηχανικών Πληροφοριακών και

Επικοινωνιακών Συστημάτων

Πανεπιστήμιο Αιγαίου

Αναπληρωτής Καθηγητής Λαμπρινουδάκης Κωνσταντίνος, Μέλος

Τμήμα Ψηφιακών Συστημάτων

Πανεπιστήμιο Πειραιά

Επίκουρος Καθηγητής Κοκολάκης Σπυρίδων, Μέλος

Τμήμα Μηχανικών Πληροφοριακών και

Επικοινωνιακών Συστημάτων

Πανεπιστήμιο Αιγαίου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΣΑΜΟΣ 2013

ΕΠΤΑΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ
ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ

Καθηγητής Γκρίτζαλης Στέφανος

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Πανεπιστήμιο Αιγαίου

Αναπληρωτής Καθηγητής Λαμπρινουδάκης Κωνσταντίνος

Τμήμα Ψηφιακών Συστημάτων

Πανεπιστήμιο Πειραιά

Επίκουρος Καθηγητής Κοκολάκης Σπυρίδων

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Πανεπιστήμιο Αιγαίου

Επίκουρος Καθηγητής Ριζομυλιώτης Παναγιώτης

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Πανεπιστήμιο Αιγαίου

Αναπληρωτής Καθηγητής Κάτος Βασίλειος

Τμήμα Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Δημοκρίτειο Πανεπιστήμιο Θράκης

Επίκουρος Καθηγητής Μαριάς Ιωάννης

Τμήμα Πληροφορικής

Οικονομικό Πανεπιστήμιο Αθηνών

Επίκουρος Καθηγητής Καλλονιάτης Χρήστος

Τμήμα Πολιτισμικής Τεχνολογίας και Επικοινωνίας

Πανεπιστήμιο Αιγαίου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΣΑΜΟΣ 2013

Οι απόψεις και τα συμπεράσματα που περιέχονται στο παρόν έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Πανεπιστημίου Αιγαίου.

ΠΕΡΙΛΗΨΗ

Η Ηλεκτρονική Διακυβέρνηση είναι άμεσα συνδεδεμένη με τη μεταρρύθμιση και τον εκσυγχρονισμό της Δημόσιας Διοίκησης μέσω της αξιοποίησης σύγχρονων τεχνολογιών και μεθοδολογιών. Για να καταστεί όμως δυνατή και επιτυχημένη μία τέτοια μετάβαση, δεν αρκεί η αυτοματοποίηση των υπαρχουσών διαδικασιών και η παροχή τους μέσω του Διαδικτύου. Η Δημόσια Διοίκηση καλείται να εγκαθιδρύσει και να διατηρήσει καθολικά ένα επίπεδο προστασίας και ασφάλειας, όχι μόνο αντίστοιχο και ισότιμο με αυτό των υπαρχουσών υπηρεσιών, αλλά ικανό να διασφαλίσει ότι τα προσωπικά δεδομένα αξιοποιούνται με τρόπο διαφανή και σύννομο, λαμβάνοντας υπ' όψιν το συμφέρον των πολιτών. Σκοπός της παρούσας διατριβής είναι η μελέτη εφαρμογής και αξιοποίησης τεχνολογιών και μεθοδολογιών προάσπισης της ιδιωτικότητας σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης, καθώς και η διαμόρφωση ενός πλαισίου για την ολοκληρωμένη διαχείριση των ψηφιακών ταυτοτήτων για όλες τις συμμετέχουσες οντότητες. Αρχικά, αποτυπώνονται οι απαιτήσεις ασφάλειας και ιδιωτικότητας σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης και καταγράφονται συγκεντρωτικά τόσο οι δυνητικές απειλές όσο και οι πιθανές επιπτώσεις τους αναφορικά με την απώλεια των προηγούμενων απαιτήσεων, και προτείνονται τρόποι αντιμετώπισης και ελαχιστοποίησής τους. Στη συνέχεια προτείνονται ολοκληρωμένες μεθοδολογίες ενσωμάτωσης και διαχείρισης τομεακών αναγνωριστικών σε ψηφιακά πιστοποιητικά X.509 v3, σε περιβάλλοντα ομόσπονδων ταυτοτήτων και σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης 2.0. Λαμβάνοντας υπ' όψιν τις απαιτήσεις και τους περιορισμούς του ελληνικού νομικού και κανονιστικού πλαισίου, προτείνεται ένα ολοκληρωμένο Πλαίσιο Ψηφιακής Αυθεντικοποίησης, μέσω του προσδιορισμού των κατάλληλων επιπέδων εμπιστοσύνης, αυθεντικοποίησης και εγγραφής των τελικών χρηστών. Τέλος, προτείνεται για πρώτη φορά μία ολοκληρωμένη αρχιτεκτονική ενσωμάτωσης και αξιοποίησης Πολιτικών και Προτιμήσεων Ιδιωτικότητας σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης, με στόχο την απλουστευμένη παροχή ηλεκτρονικών υπηρεσιών, την παροχή των απαραίτητων ελεγκτικών μηχανισμών στους χρήστες για τη συλλογή, επεξεργασία και αποθήκευση των προσωπικών τους δεδομένων, καθώς και τη διαβεβαίωση για την τήρηση των αντίστοιχων νομικών και κανονιστικών απαιτήσεων από την πλευρά των παρόχων.

Προκόπιος Δρογκάρης

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ABSTRACT

e-Government is directly related to the reform and modernization of Public Administration through the exploitation of modern technologies and methodologies. However, for such a reform it is not adequate to automate existing processes and deliver them via the Internet. Public Administration is required to establish and maintain a universal privacy and security level, not only relevant and equal to that of existing services, but suffice enough to ensure that personal data is exploited transparently and lawfully, taking into account citizens' interests. The scope of this thesis is to examine the application and utilization of applicable innovative technologies and methodologies towards improving privacy and security in e-Government Information Systems and devise a framework for integrated management of digital identities. Initially, security and privacy requirements in e-Government are depicted and the potential threats and their possible implications regarding the loss of the previous requirements are catalogued and summarized. Next, comprehensive methodologies for integration and management of sectorial identifiers in X.509 v3 digital certificates, in federated environments and in e-Government 2.0 environments are proposed. Taking into account the requirements and limitations of the Greek legal and regulatory framework an integrated and holistic Digital Authentication Framework is also proposed, through the identification of appropriate levels of trust, authentication and registration of end users. Finally, a comprehensive architecture is proposed for the first time, which integrates and exploits Privacy Policies and Preferences in e-Government environments towards the provision of simplified services and the necessary control mechanisms for users regarding the collection, processing and storage of their personal data.

Prokopios Drogkaris

Department of Information and Communication Systems Engineering

UNIVERSITY OF THE AEGEAN

ΑΦΙΕΡΩΣΕΙΣ

Αφιερωμένο στους γονείς μου, Ευαγγελία και Κωνσταντίνο.

ΕΥΧΑΡΙΣΤΙΕΣ

Ολοκληρώνοντας την μακροχρόνια προσπάθεια και φτάνοντας στην "Ιθάκη" μου δεν μπορώ παρά να συμμεριστώ τα λόγια του ποιητή:

«Σὰ βγεῖς στὸν πηγαιμὸ γιὰ τὴν Ἰθάκη,
νὰ εὔχεσαι νά 'ναι μακρὺς ὁ δρόμος,
γεμάτος περιπέτειες, γεμάτος γνώσεις.

Τοὺς Λαιστρυγόνας καὶ τοὺς Κύκλωπας,
τὸν θυμωμένο Ποσειδῶνα μὴ φοβᾶσαι,
τέτοια στὸν δρόμο σου ποτέ σου δὲν θὰ βρεῖς,
ἂν μέν' ἡ σκέψις σου ὑψηλή, ἂν ἐκλεκτὴ
συγκίνησις τὸ πνεῦμα καὶ τὸ σῶμα σου ἀγγίζει
...
Σὲ πόλεις Αἰγυπτιακὲς πολλὲς νὰ πᾷς,
νὰ μάθεις καὶ νὰ μάθεις ἀπ' τοὺς σπουδασμένους.
Πάντα στὸ νοῦ σου νά 'χεις τὴν Ἰθάκη.
Τὸ φθάσιμον ἐκεῖ εἶν' ὁ προορισμός σου…»

Ο δρόμος ήταν όντως μακρύς, γεμάτος περιπέτειες και γνώση. Είχα όμως την τύχη να έχω στο πλευρό μου αξιόλογους επιστήμονες, συνεργάτες και φίλους που με καθοδήγησαν, με εμψύχωσαν, με στήριξαν και με υπέμειναν αδιαμαρτύρητα.

Αρχικά θα ήθελα να εκφράσω ένα μεγάλο ευχαριστώ από βάθους καρδίας στον επιβλέποντα καθηγητή κ. Στέφανο Γκρίτζαλη και τον συνεπιβλέπωντα καθηγητή κ. Κώστα Λαμπρινουδάκη. Από την αρχή της γνωριμίας μας, το 2000, ως πρωτοετής φοιτητής, μέχρι σήμερα, μου προσέφεραν απλόχερα και ανιδιοτελώς επιστημονική, πνευματική και ηθική καθοδήγηση. Τους ευχαριστώ για την εμπιστοσύνη που μου έδειξαν και με τίμησαν με τη συνεργασία τους, αφιερώνοντάς μου αρκετό από το χρόνο τους. Αποτελούν πρότυπο για τη μελλοντική πορεία μου ως επιστήμονα και ευελπιστώ η συνεργασία μας να συνεχιστεί και στο μέλλον. Ιδιαίτερη ευχαριστία αξίζει και στην καθηγήτρια κ. Λίλιαν Μήτρου που με τις πολύτιμες συμβουλές, το γνήσιο ενδιαφέρον και την καλόπιστη εποικοδομητική κριτική της, συνέβαλε τα μέγιστα τόσο στην επιστημονική εξέλιξή μου όσο και στην ολοκλήρωση της παρούσας διατριβής.

Θα ήθελα επίσης να ευχαριστήσω τη σύντροφό μου Άννα – Βικτώρια που είναι στο πλευρό μου από την αρχή αυτού του ταξιδιού, δίνοντάς μου κουράγιο και δύναμη να συνεχίσω και να πετύχω τους στόχους μου. Την ευχαριστώ για την υπομονή και την ανεκτικότητα που έχει επιδείξει όλα αυτά τα χρόνια.

Δεν θα μπορούσα να μην ευχαριστήσω τους συνεργάτες στο εργαστήριο Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου και ιδιαίτερα τον Δρ. Δημήτριο Γενειατάκη για την ανεκτίμητη βοήθεια και καθοδήγησή του στα πρώτα μου βήματα ως υποψήφιος διδάκτορας. Επίσης, όλους τους φίλους, συγγενείς και τους συνεργάτες στο Πανεπιστήμιο Πειραιά, στο ΤΕΙ Πειραιά και στο Κέντρο Μελετών Ασφάλειας για τις εποικοδομητικές συζητήσεις, την υποστήριξη, την κατανόηση και την ανοχή που έδειξαν όλα αυτά τα χρόνια στις προτεραιότητες και στις επιλογές μου. Ο καθένας του έχει συμβάλει με το δικό του ξεχωριστό τρόπο στο να βρίσκομαι σήμερα σε αυτή τη θέση.

Τέλος, οφείλω το πιο μεγάλο ευχαριστώ στην οικογένειά μου, Ευαγγελία, Κωνσταντίνο, Ευγενία και Σωτήρη, για την αμέριστη αγάπη, υποστήριξη και συμπαράσταση καθώς και για τις θυσίες και παραχωρήσεις που έχουν κάνει. Ευελπιστώ με την παρούσα διατριβή να ικανοποιούνται οι προσδοκίες που έτρεφαν στο πρόσωπό μου.

Προκόπιος Δρογκάρης

Οκτώβριος 2013

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ 1 - ΕΙΣΑΓΩΓΗ

Στο παρόν κεφάλαιο παρέχεται μία συνολική επισκόπηση της ερευνητικής περιοχής στην οποία κινήθηκε η διεξαχθείσα έρευνα καθώς και τα κίνητρα και οι στόχοι της. Παρουσιάζεται συνολικά η επιστημονική και ερευνητική συνεισφορά της παρούσας διατριβής στα επιμέρους κεφάλαια αναφορικά με τις απαιτήσεις ασφάλειας και ιδιωτικότητας σε Πληροφορικά Συστήματα Ηλεκτρονικής Διακυβέρνησης, τη διαχείριση ψηφιακών αναγνωριστικών τελικών χρηστών, ένα ολοκληρωμένο Πλαίσιο Ψηφιακής Αυθεντικοποίησης και την αξιοποίηση πολιτικών και προτιμήσεων Ιδιωτικότητας. Τέλος, παρουσιάζεται συνοπτικά το περιεχόμενο των υπόλοιπων κεφαλαίων.

1.1 Περιγραφή Ερευνητικού Πεδίου

Η ραγδαία ανάπτυξη των Τεχνολογιών Πληροφορίας και Επικοινωνιών (ΤΠΕ) συνέβαλε στην εξάπλωση καινοτόμων εφαρμογών, όπως το Ηλεκτρονικό Εμπόριο (*e-Commerce*), η Ηλεκτρονική Μάθηση (*e-Learning*) και η Ηλεκτρονική Διακυβέρνηση (*e-Government*). Αδιαμφισβήτητα, η τελευταία είναι άμεσα συνδεδεμένη με τη μεταρρύθμιση και τον εκσυγχρονισμό της Δημόσιας Διοίκησης και γι' αυτό ο σχεδιασμός και η ανάπτυξη ηλεκτρονικών υπηρεσιών αποτελεί σημαντική προτεραιότητα. Η εμφάνιση της συγκεκριμένης έννοιας ανέδειξε την ανάγκη για χρήση και αξιοποίηση σύγχρονων τεχνολογιών και μεθοδολογιών προς την κατεύθυνση του ανασχεδιασμού των διοικητικών διαδικασιών, την αναδιοργάνωση, τη βελτίωση λειτουργίας και τον έλεγχο των παρεχόμενων υπηρεσιών, την παροχή καινούργιων διαδικασιών πρόσβασης και διάχυσης της απαραίτητης πληροφορίας, καθώς και της συνολικής σχέσης μεταξύ Δημόσιας Διοίκησης και πολιτών. Τα προσδοκώμενα αποτελέσματα από αυτή την εξέλιξη εντοπίζονται στη μείωση των γραφειοκρατικών διαδικασιών και τη μετάβαση σε μια σύγχρονη, ευέλικτη, διαφανή και αποτελεσματικότερη Δημόσια Διοίκηση, με ταυτόχρονη εξοικονόμηση πόρων, μείωση του συνολικού κόστους λειτουργίας και καλύτερη αξιοποίηση του υφιστάμενου ανθρώπινου δυναμικού.

Για να καταστεί όμως δυνατή και επιτυχημένη μία τέτοια μετάβαση δεν αρκεί η αυτοματοποίηση των υπαρχουσών διαδικασιών και η παροχή τους μέσω του Διαδικτύου ή η αυτούσια μεταφορά ενός γραφειοκρατικού συστήματος σε ηλεκτρονική μορφή απαιτείται ένας ολιστικός ανασχεδιασμός της Δημοσίας Διοίκησης, ώστε αυτή να καταστεί πραγματικά ανοιχτή (*Open*),

συνεργατική (*Collaborative*) και διαλειτουργική (*Interoperable*), παύοντας πλέον να λειτουργεί στα στενά όρια ενός τμήματος ή μεμονωμένα μιας Δημόσιας Υπηρεσίας, αξιοποιώντας παράλληλα καινοτόμες τεχνολογίες και μεθοδολογίες.

Η Δημόσια Διοίκηση καλείται να εγκαθιδρύσει και να διατηρήσει καθολικά ένα επίπεδο προστασίας και ασφάλειας, όχι μόνο αντίστοιχο και ισότιμο με αυτό των υπαρχουσών υπηρεσιών αλλά ικανό να διασφαλίσει ότι τα προσωπικά δεδομένα αξιοποιούνται με τρόπο διαφανή και σύννομο, λαμβάνοντας υπ' όψιν το συμφέρον των πολιτών. Η παροχή ηλεκτρονικών υπηρεσιών συνοδεύεται από την αποκάλυψη προσωπικών δεδομένων των πολιτών που κάνουν χρήση των υπηρεσιών, και την ηλεκτρονική συγκέντρωση και επεξεργασία σημαντικού όγκου πληροφορίας για κάθε πολίτη, η οποία μπορεί να οδηγήσει στη δημιουργία ενός εκτεταμένου προφίλ ή να διευκολύνει μη εξουσιοδοτημένη πρόσβαση στο σύνολο της πληροφορίας. Επιπρόσθετα, εξαιτίας της ενσωμάτωσης των ΤΠΕ, υπεισέρχονται καινούργιες απειλές (*Threats*) που απαιτούν τη μελέτη και εφαρμογή μηχανισμών και μεθοδολογιών ασφάλειας, ικανών να εγγυηθούν την αυθεντικότητα (*Authenticity*) της ψηφιακής ταυτότητας (*Digital Identity*) των συναλλασσόμενων, την ακεραιότητα (*Integrity*) και την εμπιστευτικότητα (*Confidentiality*) του περιεχομένου κάθε συναλλαγής, καθώς και τη μη-αποποίηση (*Non-repudiation*) συμμετοχής και ολοκλήρωσης της συναλλαγής.

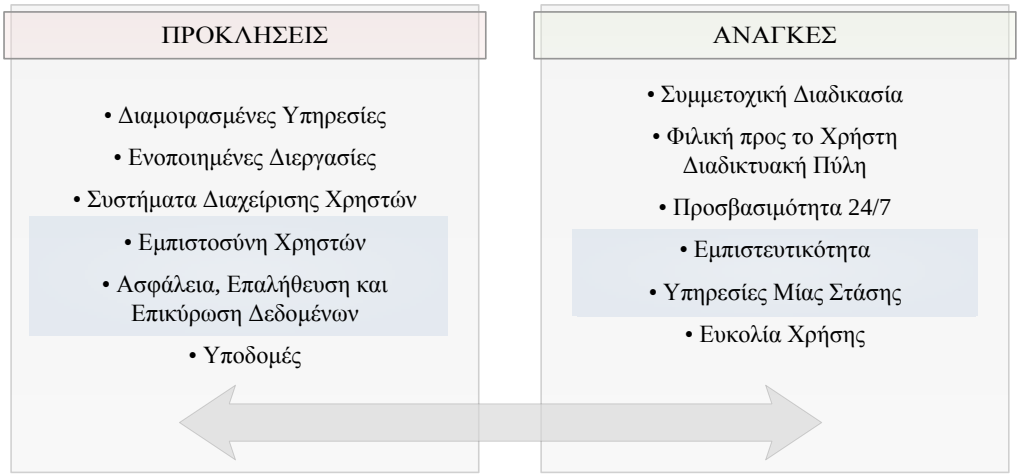
Την ικανοποίηση αυτών των απαιτήσεων έρχεται να καλύψει ένα ευρύ φάσμα Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας (*Privacy Enhancing Technologies*), που όμως δεν μπορούν από μόνες τους να διασφαλίσουν το απαιτούμενο επίπεδο εμπιστοσύνης και ασφάλειας. Αυτό που πραγματικά απαιτείται είναι η ένταξη της προστασίας της ιδιωτικότητας στα χαρακτηριστικά των προς αξιοποίηση τεχνολογιών και μεθοδολογιών τόσο στον σχεδιασμό και την αρχιτεκτονική των υπό-ανάπτυξη Πληροφοριακών Συστημάτων Ηλεκτρονικής, όσο και στο σύνολο των επιχειρησιακών διαδικασιών και πρακτικών, προς την κατεύθυνση της Ιδιωτικότητας εκ σχεδίου και διά σχεδιασμού (*Privacy By Design*).

1.2 Κίνητρα και Στόχοι Έρευνας

Οι εκθέσεις των Ηνωμένων Εθνών για την ανάπτυξη της Ηλεκτρονικής Διακυβέρνησης σε παγκόσμιο επίπεδο από το 2001 έως το 2012 (United Nations, 2013), αποτελούν μια συντονισμένη προσπάθεια για την καταγραφή, αποτύπωση και αποτίμηση των βημάτων που έχουν πραγματοποιηθεί προς τη συγκεκριμένη κατεύθυνση. Σε κάθε μία παρέχονται πληροφορίες σχετικά με

τις διαφορετικές στρατηγικές ανάπτυξης που επιλέγει να υλοποιήσει κάθε κυβέρνηση, καθώς και κοινά θέματα σχεδιασμού και υλοποίησης που άπτονται κάθε προσπάθειας. Η χρήση διευρυμένων μοντέλων για τη χρήση και αξιοποίηση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, αναγνωρίζει και αποτυπώνει τις χώρες που κατέχουν ηγετική θέση στην προώθηση και ανάπτυξη ηλεκτρονικών υπηρεσιών καθώς και εκείνες που δεν έχουν αξιοποιήσει ακόμα όλες τις δυνατότητες των ΤΠΕ.

Στο μοντέλο που χρησιμοποιήθηκε για την αξιολόγηση της υπάρχουσας κατάστασης (United Nations, 2005), αναγνωρίζονται συγκεκριμένες προκλήσεις και ανάγκες που, σε παγκόσμιο επίπεδο, θα πρέπει να ικανοποιηθούν και να αντιμετωπιστούν από όλες τις εμπλεκόμενες οντότητες, ώστε να υπάρξει πραγματική πρόοδος και εξέλιξη. Οι βασικές προκλήσεις και ανάγκες αποτυπώνονται στο Σχήμα 1-1 που ακολουθεί.



Σχήμα 1-1: Προκλήσεις και Ανάγκες Ηλεκτρονικής Διακυβέρνησης (United Nations, 2005)

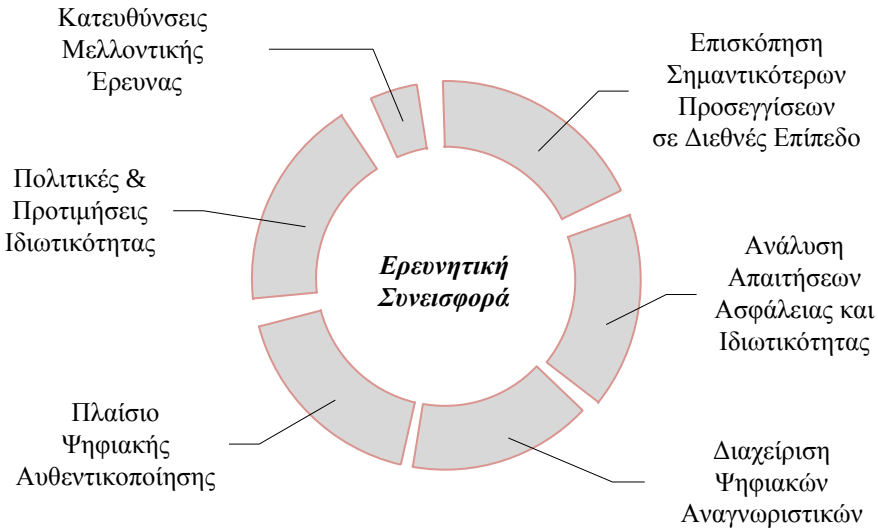
Σημαντική θέση και στους δύο άξονες κατέχουν χαρακτηριστικά που σχετίζονται με το επίπεδο εμπιστοσύνης (*Trust*) των τελικών χρηστών, την ασφάλεια (*Security*), επαλήθευση (*Verification*) και επικύρωση (*Validation*) των μεταφερόμενων δεδομένων, την εμπιστευτικότητα (*Confidentiallity*) των παρεχόμενων ηλεκτρονικών υπηρεσιών καθώς και την παροχή υπηρεσιών μιας στάσης (*One-Stop Shop)*. Παράλληλα με τις συγκεκριμένες εκθέσεις, το ζήτημα της ασφάλειας και της ιδιωτικότητας των δεδομένων που αξιοποιούνται από ένα Π.Σ. Ηλεκτρονικής Διακυβέρνησης έχει επισημανθεί και σε αρκετές αναφορές και επιστημονικές δημοσιεύσεις (Muir & Oppenheim, 2002), (Gritzalis & Lambrinoudakis, 2002), (Rezgui et al., 2002), (Lambrinoudakis et

al., 2003), (Ndou, 2004), (Dutton et al., 2005), (Layton, 2006). Οι ηλεκτρονικά παρεχόμενες υπηρεσίες δεν θεωρούνται επαρκώς ασφαλείς και οι χρήστες αποφεύγουν να τις χρησιμοποιούν, προκειμένου να μην αποστείλουν προσωπικά δεδομένα (ευαίσθητα και μη), που ενδέχεται να χρησιμοποιηθούν για σκοπούς πέραν αυτών για τους οποίους έχουν δώσει τη συγκατάθεσή τους (*Consen*t) ή καταστούν διαθέσιμα σε μη-εξουσιοδοτημένους κακόβουλους χρήστες. (ENISA, 2010)

Στόχος της έρευνας ήταν η ολοκληρωμένη καταγραφή των απαιτήσεων ασφάλειας και ιδιωτικότητας σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης και η αξιοποίηση και μελέτη εφαρμογής τεχνολογιών και μεθοδολογιών ικανών να αντιμετωπίσουν και να μειώσουν τις προσδιορισμένες απειλές και επιπτώσεις διασφαλίζοντας το απαιτούμενο επίπεδο εμπιστοσύνης.

1.3 Συνεισφορά Έρευνας

Η συνεισφορά της παρούσας διατριβής εντοπίζεται στη μελέτη εφαρμογής και αξιοποίησης τεχνολογιών και μεθοδολογιών προάσπισης της ιδιωτικότητας σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης, καθώς και στη διαμόρφωση ενός πλαισίου για την ολοκληρωμένη διαχείριση ψηφιακών ταυτοτήτων για όλες τις συμμετέχουσες οντότητες. Η συνεισφορά της έρευνας ανά θεματική περιοχή παρουσιάζεται στο Σχήμα 1-2 παρακάτω.



Σχήμα 1-2: Συνεισφορά Έρευνας

Αρχικό στάδιο της έρευνας αποτέλεσε η μελέτη, καταγραφή και ανάλυση των σημαντικότερων προσεγγίσεων σε Κράτη-Μέλη της Ευρωπαϊκής Ένωσης, όπως το Ηνωμένο Βασίλειο και η Ιρλανδίας, αλλά και σε κράτη εκτός αυτής, όπως η Αυστραλία, οι Η.Π.Α. και η Νέα Ζηλανδία. Η επισκόπηση αφορούσε στο συνολικό στρατηγικό σχεδιασμό για την ανάπτυξη και προώθηση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, καθώς επίσης και στα πλαίσια διαλειτουργικότητας (*Interoperability*), ασφάλειας (*Security*) και ψηφιακής αυθεντικοποίησης (*Digital Authentication*) [D1]. Τα στοιχεία που προέκυψαν από την καταγραφή. Έχουν αποτελέσει το γνωστικό υπόβαθρο για την μετέπειτα έρευνα.

Επόμενο βήμα αποτέλεσε η καταγραφή των απαιτήσεων ασφάλειας και ιδιωτικότητας σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης, σε επίπεδο τελικών χρηστών, παρόχων ηλεκτρονικών υπηρεσιών καθώς και το ισχύον νομικό και κανονιστικό πλαίσιο. Η επισκόπηση και καταγραφή των σημαντικότερων προσεγγίσεων, ύστερα από πρωτογενή και δευτερογενή έρευνα, ανέδειξε την έλλειψη μιας ολοκληρωμένης προσέγγισης, που να λαμβάνει υπόψη τόσο τις τεχνολογικές απαιτήσεις όσο και τους περιορισμούς που υπαγορεύονται από το νομικό και κανονιστικό πλαίσιο. Εν συνεχεία, αναγνωρίστηκαν και καταγράφηκαν συγκεντρωτικά τόσο οι δυνητικές απειλές όσο και οι πιθανές επιπτώσεις τους σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης αναφορικά με την απώλεια των προηγούμενων απαιτήσεων, και προτάθηκαν τρόποι αντιμετώπισης και ελαχιστοποίησής τους [D1]. Η συγκροτημένη καταγραφή τους συνέβαλε στην αξιολόγηση των μετέπειτα προτάσεων όσον αφορά στην προάσπιση της ιδιωτικότητας των τελικών χρηστών.

Δεδομένης της ιδιαίτερης σημασίας συσχέτισης - αντιστοίχισης της πραγματικής ταυτότητας του τελικού χρήστη με συγκεκριμένη ψηφιακή ταυτότητα και της διαχείρισής της, καθ' όλη τη διάρκεια του κύκλου ζωής τους, εξετάστηκαν οι διαφορετικές πρακτικές-μεθοδολογίες ταυτοποίησης και διασύνδεσης μερικών ψηφιακών ταυτοτήτων [D1]. Με βάση το RFC 4683, προτάθηκε μία αποτελεσματική και επικεντρωμένη στο χρήστη μεθοδολογία για την αποθήκευση πολλαπλών αναγνωριστικών σε ψηφιακά πιστοποιητικά X.509 v3. Η συγκεκριμένη μέθοδος επιτρέπει την απρόσκοπτη ταυτοποίηση του χρήστη σε διαφορετικά περιβάλλοντα, όπου δεν είναι δυνατή η αξιοποίηση ενός μοναδικού καθολικού αναγνωριστικού [C2]. Παράλληλα, προτάθηκε μία ολοκληρωμένη μεθοδολογία ενσωμάτωσης και διαχείρισης τομεακών αναγνωριστικών τελικών χρηστών τόσο σε περιβάλλοντα ομόσπονδων ταυτοτήτων (*Federated Identities*) [C4] όσο και σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης 2.0 [C3], προκειμένου να καταστεί δυνατή η ενιαία πρόσβαση σε ηλεκτρονικές υπηρεσίες. Τέλος, μελετήθηκαν και αποτυπώθηκαν οι νέες προκλή-

σεις στη διαχείριση των ψηφιακών ταυτοτήτων, που προκύπτουν σε διασυνδεμένα νεφοϋπολογιστικά συστήματα (*Cloud Computing*) [C1].

Η ευρεία αποδοχή των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης εξαρτάται σε μεγάλο βαθμό από το επίπεδο εμπιστοσύνης και βεβαιότητας που δημιουργείται στους χρήστες για τις παρεχόμενες ηλεκτρονικές υπηρεσίες, καθώς και από το συνολικό επίπεδο ασφάλειας. Προς αυτή την κατεύθυνση προτάθηκε ένα ολοκληρωμένο Πλαίσιο Ψηφιακής Αυθεντικοποίησης, μέσω του προσδιορισμού κατάλληλων επιπέδων εμπιστοσύνης, αυθεντικοποίησης και εγγραφής των τελικών χρηστών [D1], [C6]. Ανάλογα με το είδος των δεδομένων που αξιοποιούνται σε κάθε ηλεκτρονική συναλλαγή με ένα δημόσιο φορέα, προτάθηκαν οι αντίστοιχες διαδικασίες εγγραφής και αυθεντικοποίησης, ώστε να ικανοποιούνται οι εκάστοτε απαιτήσεις ασφάλειας και ιδιωτικότητας. Επιπλέον, προτάθηκε μια αρχιτεκτονική ενιαίας πρόσβασης, καθώς και οι απαραίτητοι κανόνες και οδηγίες που θα πρέπει να τηρούνται τόσο από τους τελικούς χρήστες όσο και από τους Δημόσιους Φορείς. Κατά το σχεδιασμό λήφθηκαν υπόψη οι απαιτήσεις και οι περιορισμοί του ελληνικού νομικού και κανονιστικού πλαισίου, προκειμένου αυτό να μπορεί να εφαρμοστεί στην Ελληνική Δημόσια Διοίκηση.

Η συνεχώς αυξανόμενη απαίτηση των τελικών χρηστών για έλεγχο των προσωπικών τους δεδομένων που αξιοποιούνται από υπηρεσίες Ηλεκτρονικής Διακυβέρνησης, οδήγησε στην μελέτη και αξιοποίηση των Πολιτικών και των Προτιμήσεων ιδιωτικότητας (*Privacy Policies and Privacy Preferences*). Παρ' όλη την εξάπλωσή τους σε εφαρμογές Ηλεκτρονικού Εμπορίου, δεν είχε υπάρξει ανάλογη μελέτη σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης. Με βάση τις απαιτήσεις ιδιωτικότητας, προτείνεται για πρώτη φορά μία ολοκληρωμένη αρχιτεκτονική ενσωμάτωσης και αξιοποίησής τους, [C5], [J1], [J2]. Στόχος της συγκεκριμένης αρχιτεκτονικής είναι να απλουστεύσει την παροχή ηλεκτρονικών υπηρεσιών, να παράσχει στους τελικούς χρήστες τον απαραίτητο έλεγχο για τη συλλογή, επεξεργασία και αποθήκευση των προσωπικών τους δεδομένων, καθώς και τη διαβεβαίωση για την τήρηση των αντίστοιχων νομικών και κανονιστικών υποχρεώσεων από την πλευρά των παρόχων. Η συγκεκριμένη αρχιτεκτονική βασίστηκε στις απαιτήσεις ιδωτικότητας και στο μοντέλο που προτάθηκε στο [C6].

Ο Πίνακας 1-1 παρακάτω συνοψίζει τη συνεισφορά της παρούσας διατριβής ανά κεφάλαιο.

Κεφάλαια	Περιγραφή Κεφαλαίου	Συνεισφορά	Περιγραφή Συνεισφοράς
Κεφάλαιο 1	Εισαγωγή		-
Κεφάλαιο 2	Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης	D1	Επισκόπηση σημαντικότερων προσεγγίσεων Ηλεκτρονικής Διακυβέρνησης
Κεφάλαιο 3	Απαιτήσεις Ασφάλειας και Ιδιωτικότητας	D1	Καταγραφή Απαιτήσεων Ασφάλειας και Ιδιωτικότητας σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης
Κεφάλαιο 4	Ψηφιακά Αναγνωριστικά	C1, C2, C3, C4, D1	Πρόταση ολοκληρωμένων μεθόδων ενσωμάτωσης και διαχείρισης τομεακών αναγνωριστικών τελικών χρηστών σε περιβάλλοντα: • Ομόσπονδων ταυτοτήτων και • Ηλεκτρονικής Διακυβέρνησης 2.0 και • Αποθήκευση σε ψηφιακά πιστοποιητικά X.509 v3.
Κεφάλαιο 5	Πλαίσιο Ψηφιακής Αυθεντικοποίησης	D1, C6	Ολοκληρωμένο πλαίσιο ψηφιακής αυθεντικοποίησης για την εγκαθίδρυση και διασφάλιση των απαιτούμενων επιπέδων εμπιστοσύνης στις παρεχόμενες ηλεκτρονικές υπηρεσίες.
Κεφάλαιο 6	Πολιτικές και Προτιμήσεις Ιδιωτικότητας	C5, J1, J2	Ολοκληρωμένη αρχιτεκτονική ενσωμάτωσης και αξιοποίησης πολιτικών και προτιμήσεων ιδιωτικότητας σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης
Κεφάλαιο 7	Συμπεράσματα		-

Πίνακας 1-1: Συνεισφορά Διατριβής ανά Κεφάλαιο

1.3.1 Ερευνητικές – Επιστημονικές Δημοσιεύσεις[1]

Σε Διεθνή Επιστημονικά Περιοδικά μετά από Πλήρη Κρίση

J1 P. Drogkaris, S. Gritzalis, C. Lambrinoudakis, "*Employing Privacy Policies and Preferences in Modern e-Government Environments*", Special Issue on "Security and Privacy of E-Government Applications and Services" of the International Journal of Electronic Governance, 2013, Inderscience Publishers ***(0)***

J2 P. Drogkaris, S. Gritzalis, C. Lambrinoudakis, "*A Hierarchical Multitier Approach for Privacy Policies in e-Government Environments*", the International Journal of Electronic Governance, (Under Review) , Inderscience Publishers ***(0)***

Σε Διεθνή Επιστημονικά Συνέδρια μετά από Πλήρη Κρίση

C1 D. Núñez, I. Agudo, P. Drogkaris, S. Gritzalis, "Identity Management Challenges for Intercloud Applications", 1st International Workshop on Security & Trust for Applications in Virtualised Environments (STAVE 2011), C. Skianis, (Ed.), pp. 198 - 204, June, 2011, Loutraki, Greece, Communications in Computer and Information Science Series CCIS, Springer ***(4)***

C2 P. Drogkaris, S. Gritzalis, "*Attaching Multiple Personal Identifiers in X.509 Digital Certificates*", EuroPKI 2010 7th European Workshop on Public Key Services, Applications and Infrastructures, J. Camenisch and C. Lambrinoudakis, (Eds.), pp. 171-177, September 2010, Athens, Greece, Lecture Notes in Computer Science LNCS, Springer ***(0)***

C3 P. Drogkaris, S. Gritzalis, C. Lambrinoudakis, "*Transforming the Greek e-Government Environment towards the e-Gov 2.0 Era*", EGOVIS'10 International Conference on Electronic Government and the Information Systems Perspective, K. Andersen, E. Francesconi, A. Gronlund, T. M. Engers. (Eds.), pp. 142 -149, September 2010, Bilbao, Spain, Lecture Notes in Computer Science LNCS, Springer ***(5)***

[1] Ο αριθμός στην παρένθεση υποδηλώνει τον αριθμό των ετεροαναφορών ανά δημοσίευση από μη συνεργάτες

C4 P. Drogkaris, C. Lambrinoudakis, S. Gritzalis, "*Introducing Federated Identities to One-Stop-Shop e-Government Environments: The Greek Case*", eChallenges 2009 19th Conference, P. Cunningham, M. Cunningham (Eds.), pp. 115 – 121, October 2009, Istanbul, Turkey, eChallenges e-2009 Conference Proceedings ***(0)***

C5 P. Drogkaris, S. Gritzalis, C. Lambrinoudakis, "*Enabling Secure Data Management in e-Government Environments: The Greek Case*", EGOV'09 8th International Conference on Electronic Government, EGOV 2009, H. J. Scholl, M. Janssen, R. Traunmüller, M. A. Wimmer (Eds.), pp. 138-145, September 2009, Linz, Austria, Trauner Verlag Schriftenreihe Informatik ***(0)***

C6 P. Drogkaris, D. Geneiatakis, S. Gritzalis, C. Lambrinoudakis, L. Mitrou, "Towards an Enhanced Authentication Framework for eGovernment Services: The Greek Case", EGOV'08 7th International Conference on Electronic Government, E. Ferro, J. Scholl, M. Wimmer (Eds.), pp. 189-196, September 2008, Torino, Italy, Trauner Verlag Schriftenreihe Informatik ***(6)***

Παραδοτέα Χρηματοδοτούμενων Ερευνητικών - Μελετητικών Έργων

D1 Παραδοτέο ΠΑ1.7: Δ' Έκδοση Πλαισίου Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, Τεύχος Γ, Πλαίσιο Ψηφιακής Αυθεντικοποίησης. 2009, Κοινωνία της Πληροφορίας ΑΕ - Υπουργείο Εσωτερικών Δημόσιας Διοίκησης και Αποκέντρωσης - PLANET ΑΕ, ΕΠΙΣΕΥ/ΕΜΠ, ΑΤC - Πανεπιστήμιο Αιγαίου -

1.4 Δομή της Διατριβής

Η παρούσα διατριβή απαρτίζεται από 7 κεφάλαια, τα οποία δομούνται ως εξής:

- Στο Κεφάλαιο 1 παρέχεται μια επισκόπηση της γνωστικής περιοχής, του σκοπού, της διατριβής, των επιστημονικών και ερευνητικών συνεισφορών καθώς και η δομή της.
- Στο Κεφάλαιο 2 μελετάται και αποτυπώνεται συνοπτικά η έννοια της Ηλεκτρονικής Διακυβέρνησης, με την παράθεση των σημαντικότερων ορισμών. Στη συνέχεια παρουσιάζονται οι βασικές αρχές, οι τομείς, καθώς και τα διαφορετικά επίπεδα στα οποία μπορεί να ενταχθεί μία ηλεκτρονική υπηρεσία. Ακόμη

παρουσιάζεται η εξέλιξη των ηλεκτρονικά παρεχόμενων υπηρεσιών σε παγκόσμιο επίπεδο, καθώς και η υπάρχουσα κατάσταση στην Ελλάδα τόσο σε επίπεδο ηλεκτρονικών υπηρεσιών όσο και σε επίπεδο νομικού και κανονιστικού πλαισίου.

- Στο Κεφάλαιο 3 εξετάζεται η έννοια της Ιδιωτικότητας Πληροφοριών, η ανάγκη προάσπισής της σε Πληροφορικά Συστήματα Ηλεκτρονικής Διακυβέρνησης, καθώς και το νομικό και κανονιστικό πλαίσιο σε Ευρωπαϊκό και Εθνικό επίπεδο. Στη συνέχεια καταγράφονται και επισκοπούνται ολοκληρωμένα, ύστερα από πρωτογενή και δευτερογενή έρευνα, οι βασικές παράμετροι για την ανάλυση - αποτίμηση της επικινδυνότητας (*Risk Assessment*), μέσω της ανάλυσης τόσο των δυνητικών απειλών (*Threats*) που υφίστανται οι συναλλαγές των πολιτών και των επιχειρήσεων σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης, όσο και των αρνητικών επιπτώσεων (*Impact*) που μπορούν να προκληθούν στον πάροχο της υπηρεσίας ή και στον τελικό χρήστη.
- Στο Κεφάλαιο 4 αναλύονται διεξοδικά η συσχέτιση της πραγματικής ταυτότητας του τελικού χρήστη με την ψηφιακή του ταυτότητα, τα συστήματα διαχείρισής της καθώς και οι διαφορετικές πρακτικές-μεθοδολογίες ταυτοποίησης και διασύνδεσης μερικών ψηφιακών ταυτοτήτων. Επιπρόσθετα προτείνονται μεθοδολογίες, αποθήκευση πολλαπλών αναγνωριστικών σε ψηφιακά πιστοποιητικά X.509 v3, ενσωμάτωσης και διαχείρισης τομεακών αναγνωριστικών τελικών χρηστών σε περιβάλλοντα ομόσπονδων ταυτοτήτων καθώς και σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης 2.0. Τέλος, αποτυπώνονται και οι προκλήσεις διαχείρισης των ψηφιακών ταυτοτήτων σε νεφοϋπολογιστικά συστήματα Ηλεκτρονικής Διακυβέρνησης.
- Στο Κεφάλαιο 5 παρουσιάζεται και προτείνεται ένα ολοκληρωμένο Πλαίσιο Ψηφιακής Αυθεντικοποίησης, που αποσκοπεί στη θέσπιση κανόνων και οδηγιών για την ιεράρχηση της κρισιμότητας κάθε ηλεκτρονικής υπηρεσίας και την επιλογή των μηχανισμών αυθεντικοποίησης και εγγραφής, με τρόπο σαφή, απλό, μεθοδικό και τεκμηριωμένο. Οι κανόνες και οι οδηγίες του βασίζονται στο ισχύον εθνικό νομικό και κανονιστικό πλαίσιο για την προστασία των προσωπικών και ευαίσθητων προσωπικών δεδομένων, καθώς και στην προάσπιση της ιδιωτικότητας των πολιτών.

- Στο Κεφάλαιο 6 εξετάζεται για πρώτη φορά η αξιοποίηση των Πολιτικών και των Προτιμήσεων Ιδιωτικότητας σε σύγχρονα Π.Σ. Ηλεκτρονικής Διακυβέρνησης και προτείνεται μία ολοκληρωμένη αρχιτεκτονική ενσωμάτωσης, με στόχο την απλούστευση παροχής ηλεκτρονικών υπηρεσιών, διασφαλίζοντας παράλληλα ότι οι τελικοί χρήστες διατηρούν τον απαραίτητο έλεγχο για τη συλλογή, επεξεργασία και αποθήκευση των προσωπικών τους δεδομένων, καθώς και τη διαβεβαίωση για την τήρηση των αντίστοιχων νομικών και κανονιστικών υποχρεώσεων από την πλευρά των παρόχων.
- Στο Κεφάλαιο 7 επιχειρείται μία συνολική αποτίμηση της παρούσας διατριβής. Συνοψίζονται τα ερευνητικά αποτελέσματα και αποτυπώνονται δύο βασικές κατευθύνσεις για περαιτέρω έρευνα στην ευρύτερη περιοχή της ασφάλειας και προάσπισης της ιδιωτικότητας σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης.

ΚΕΦΑΛΑΙΟ 2 - ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Στο παρόν κεφάλαιο μελετάται και αποτυπώνεται συνοπτικά η έννοια της Ηλεκτρονικής Διακυβέρνησης, με την παράθεση των σημαντικότερων ορισμών. Στη συνέχεια παρουσιάζονται οι βασικές αρχές, οι τομείς, καθώς και τα διαφορετικά επίπεδα στα οποία μπορεί να ενταχθεί μία ηλεκτρονική υπηρεσία. Ακόμη παρουσιάζεται η εξέλιξη των ηλεκτρονικά παρεχόμενων υπηρεσιών σε παγκόσμιο επίπεδο, καθώς και η υπάρχουσα κατάσταση στην Ελλάδα τόσο σε επίπεδο ηλεκτρονικών υπηρεσιών όσο και σε επίπεδο νομικού και κανονιστικού πλαισίου.

2.1 Ηλεκτρονική Διακυβέρνηση

Ο όρος «Ηλεκτρονική Διακυβέρνηση» (ΗΔ) (*electronic Government – e-Government*) χρησιμοποιείται για να περιγράψει τη χρήση και εφαρμογή Τεχνολογιών Πληροφοριών και Επικοινωνιών (ΤΠΕ) σε διαδικασίες και υπηρεσίες της Δημόσιας Διοίκησης. Η χρήση τους δεν μπορεί να θεωρηθεί ως κάτι καινούργιο ή καινοτόμο, καθώς εφαρμόζεται αρκετές δεκαετίες τώρα σε διάφορους επιμέρους τομείς ή διαδικασίες της Δημόσιας Διοίκησης. Ο συγκεκριμένος όρος μπορεί να εμφανίστηκε στα τέλη της δεκαετίας του 1990, αλλά η αλληλεπίδραση προϋπήρχε, σχεδόν από την εμφάνιση των πρώτων Πληροφοριακών Συστημάτων (Grönlund & Horan, 2005) & (Danziger & Andersen, 2002)

Μια τυπική υπηρεσία Ηλεκτρονικής Διακυβέρνησης έχει τα ακόλουθα χαρακτηριστικά, τα οποία τη διαφοροποιούν από μία διαδικασία ή απλή διεργασία ενός φορέα (Διακονικολάου & Μυλωνόπουλος, 2004), (ΚτΠ, 2008).

- *Έχει τελικό χρήστη*: Ο χρήστης μπορεί να είναι πολίτης, επιχείρηση ή άλλος φορέας της Δημόσιας Διοίκησης.
- *Έχει τελικό παραδοτέο*: Το τελικό παραδοτέο πρέπει να είναι αυτοτελές και ο τελικός χρήστης που το παραλαμβάνει να είναι σε θέση να το αξιοποιήσει χωρίς να απαιτούνται επιπλέον διεργασίες ή συναλλαγές.
- *Έχει πάροχο*: Ο πάροχος της υπηρεσίας είναι μία μονάδα της Δημόσιας Διοίκησης που είναι αρμόδια για την παροχή της ηλεκτρονικής υπηρεσίας.

- *Έχει ρυθμιστή*: Ο ρυθμιστής της υπηρεσίας είναι μία, κατ' ελάχιστον, μονάδα της Δημόσιας Διοίκησης, αρμόδια για το ρυθμιστικό πλαίσιο της ηλεκτρονικής υπηρεσίας.

Αντίστοιχα, στο άρθρο 4 της Οδηγίας 2006/123/ΕΚ "Σχετικά με τις υπηρεσίες στην Εσωτερική Αγορά" δίνονται οι εξής ορισμοί:

- Ο όρος Υπηρεσία αναφέρεται στην παροχή ενός συγκεκριμένου αποτελέσματος που επιθυμεί να λάβει ένας πολίτης ή μια επιχείρηση από έναν οργανισμό του Δημόσιου Τομέα.
- Η ολοκλήρωση μιας Υπηρεσίας συνίσταται στην εκτέλεση των διαδικασιών που απαιτούνται.
- Οι Αιτούντες – Αποδέκτες μπορεί να είναι είτε φυσικά είτε νομικά πρόσωπα
  Οι Φορείς της Δημόσιας Διοίκησης παρέχουν υπηρεσίες προς τους Αιτούντες – Αποδέκτες.
- Ο Αρμόδιος Φορέας για την εκτέλεση μιας υπηρεσίας μπορεί να ορίζεται μονοσήμαντα από τη φύση και τα στοιχεία μιας υπηρεσίας.

2.1.1 Ορισμός Ηλεκτρονικής Διακυβέρνησης

Εξαιτίας της πληθώρας και ποικιλομορφίας των προσεγγίσεων της Ηλεκτρονικής Διακυβέρνησης ανά τον κόσμο, η καθιέρωση ενός ενιαίου, καθολικού και λειτουργικού ορισμού, αποδεικνύεται εξαιρετικά δύσκολη. Τα τελευταία χρόνια έχουν διατυπωθεί διάφοροι ορισμοί για τον συγκεκριμένο όρο· κάποιοι εστιάζουν περισσότερο στη χρήση και αξιοποίηση των ΤΠΕ, ενώ κάποιοι το αντιμετωπίζουν υπό την ευρύτερη έννοια του μετασχηματισμού της παραδοσιακής διακυβέρνησης. Οι πλέον ευρέως αποδεκτοί ορισμοί που έχουν διατυπωθεί μέχρι σήμερα, παρατίθενται στη συνέχεια:

- Ευρωπαϊκή Επιτροπή: ΗΔ είναι "*Η χρήση των τεχνολογιών της πληροφορικής και των τηλεπικοινωνιών στη Δημόσια Διοίκηση, σε συνδυασμό με οργανωτικές αλλαγές και νέες δεξιότητες του προσωπικού, με σκοπό την βελτίωση της εξυπηρέτησης του κοινού, την ενδυνάμωση της δημοκρατίας και την υποστήριξη των δημόσιων πολιτικών*".
- Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ): ΗΔ είναι "*Η χρήση από την κυβέρνηση εφαρμογών Διαδικτύου και άλλων τεχνολογιών, σε*

συνδυασμό με διαδικασίες που ενσωματώνουν αυτές τις τεχνολογίες για την ενίσχυση της πρόσβασης στην κρατική πληροφορία και υπηρεσία προς το κοινό, άλλες υπηρεσίες και κρατικές οντότητες, ή την βελτίωση σε κυβερνητικές λειτουργίες ως προς την αποτελεσματικότητα, την ποιότητα των υπηρεσιών και τον μετασχηματισμό τους".

- Ευρωπαϊκό Παρατηρητήριο για την Τεχνολογία Πληροφορίας: "*Η Ηλεκτρονική Διακυβέρνηση ορίζεται ως η χρήση των τεχνολογιών Διαδικτύου στη διεξαγωγή, ενίσχυση και υποστήριξη των σχέσεων μεταξύ κυβερνητικών φορέων, πολιτών και επιχειρήσεων*".
- Ηνωμένα Έθνη: "*Η Ηλεκτρονική Διακυβέρνηση ορίζεται ως η αξιοποίηση του Διαδικτύου και του Παγκόσμιου Ιστού για την ηλεκτρονική παροχή πληροφοριών και υπηρεσιών στους πολίτες*".

Συνολικά, τα κοινά τους σημεία μπορούν να συνοψιστούν στα παρακάτω χαρακτηριστικά:

- Παροχή υπηρεσιών που βασίζονται στις τεχνολογίες Διαδικτύου
- Αξιοποίηση των ΤΠΕ σε όλες τις δραστηριότητες της Δημόσιας Διοίκησης
- Μετασχηματισμός διαδικασιών της Δημόσιας Διοίκησης

2.1.2 Βασικές Αρχές Ανάπτυξης Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Σύμφωνα με την αναφορά των Ηνωμένων Εθνών (United Nations, 2003), οι βασικές αρχές (*Principles*) για την ανάπτυξη ενός ολοκληρωμένου και επιτυχημένου περιβάλλοντος Ηλεκτρονικής Διακυβέρνησης είναι:

- υποστήριξη, δέσμευση και συμμετοχή της κεντρικής κυβέρνησης στον στρατηγικό σχεδιασμό και την υλοποίηση των στόχων,
- αποτελεσματικότητα και αποδοτικότητα της κεντρικής κυβέρνησης στην υλοποίηση των απαιτούμενων αλλαγών,
- διασφάλιση απαιτούμενης και επαρκούς χρηματοδότησης,
- καλλιέργεια και ανάπτυξη της απαραίτητης κουλτούρας στη Δημόσια Διοίκηση,
- προγραμματισμός και συντονισμός των απαιτούμενων δράσεων,
- διαμόρφωση κατάλληλου νομικού και κανονιστικού πλαισίου,

- συνεχής παρακολούθηση και αξιολόγηση,
- προώθηση και ανάδειξη των πλεονεκτημάτων στο ευρύ κοινό και
- εγκαθίδρυση του απαιτούμενο επιπέδου εμπιστοσύνης.

2.1.3 Αναγκαία Χαρακτηριστικά Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Σύμφωνα με την έκθεση της Ομάδας Εργασίας ΣΤ-5 (Διακονικολάου & Μυλωνόπουλος, 2004), ο τελικός χρήστης μίας υπηρεσίας Ηλεκτρονικής Διακυβέρνησης:

- Δεν απαιτείται να γνωρίζει ή να είναι εξοικειωμένος με τον τρόπο λειτουργίας, τη δομή και τις αρμοδιότητες των οργανωτικών μονάδων της Δημόσιας Διοίκησης που εμπλέκονται για την εξυπηρέτησή του.
- Πρέπει να έρχεται σε επαφή αποκλειστικά με το σημείο εκκίνησης της υπηρεσίας (κέντρο εξυπηρέτησης, δημόσιο πληροφοριακό σύστημα) και να παραλαμβάνει το αποτέλεσμα της υπηρεσίας από ένα σημείο εξόδου, χωρίς να εμπλέκεται σε ενδιάμεσα στάδια εξυπηρέτησης (*One Stop Shop*).
- Πρέπει να έχει συνεχή ενημέρωση για τη ροή της πληροφορίας και τη λήψη των αποφάσεων που αφορούν την υπόθεση που διεκπεραιώνει ηλεκτρονικά.

Για να ικανοποιηθούν οι συγκεκριμένες απαιτήσεις, θα πρέπει οι ηλεκτρονικές υπηρεσίες να παρέχονται από ένα Π.Σ. που υπερβαίνει τα όρια ενός φορέα, καθώς και να συνδυάζει περιεχόμενο και λειτουργίες από τις επιμέρους διαδικτυακές υπηρεσίες των εμπλεκόμενων φορέων, με τρόπο διαφανή για τον τελικό χρήστη κάθε υπηρεσίας. Προς την κατεύθυνση αυτή κινούνται οι προσπάθειες για την κατασκευή διαδικτυακών πυλών ενημέρωσης και εξυπηρέτησης, που καλύπτουν ένα ευρύ φάσμα φορέων της Δημόσιας Διοίκησης (π.χ. Οικονομικές Υπηρεσίες) ή, στη βέλτιστη περίπτωση, το σύνολο της Δημόσιας Διοίκησης. Οι διαδικτυακές αυτές πύλες είναι γνωστές με τον όρο Κυβερνητικές Δικτυακές Πύλες (*e-Government Portals*). Οι κυριότερες από αυτές παρουσιάζονται στον Πίνακας 2-1 που ακολουθεί.

Χώρα	Διαδικτυακή Πύλη	Σύνδεσμος
Αυστραλία	Government Portal	www.australia.gov.au
Αυστρία	Government Information Portal	http://help.gv.at
Γαλλία	Service-Public Portal	www.service-public.fr
Γερμανία	Service Portal of the Federal Government	www.bund.de
Ελβετία	Governmental Information & Links	www.ch.ch
Ελλάδα	Διαδικτυακή Πύλη Ερμής	www.ermis.gov.gr
Ηνωμένες Πολιτείες Αμερικής	U.S. Government's Official web portal	www.firstgov.gov
Ηνωμένο Βασίλειο	UK Government On-line	www.gov.uk
Καναδάς	Government of Canada Portal	www.canada.gc.ca
Νέα Ζηλανδία	Government Portal	www.newzealand.govt.nz
Ολλανδία	Integrated Government Portal	www.overheid.nl
Ταϊβάν	Taiwan Government Entry Point	www.taiwan.gov.tw
Χονκ Κονγκ	Hong Kong Government Services	www.gov.hk

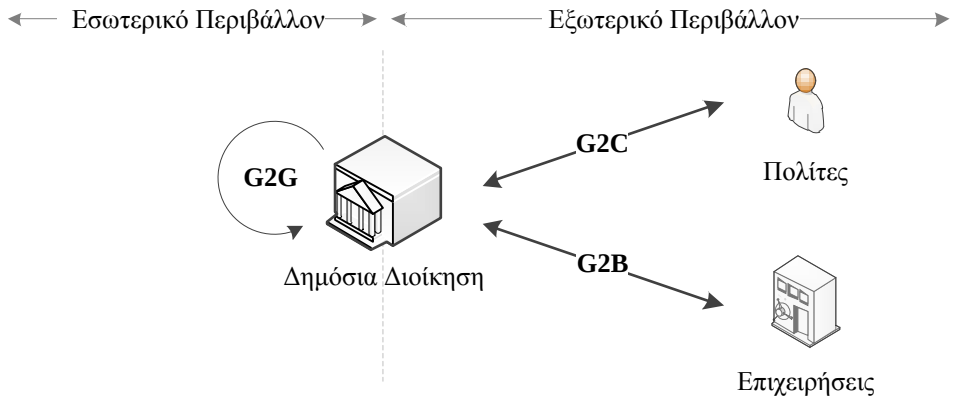
Πίνακας 2-1: Παραδείγματα Διαδικτυακών Πυλών ανά τον Κόσμο

2.1.4 Βασικοί Τομείς Ηλεκτρονικής Διακυβέρνησης

Η Ηλεκτρονική Διακυβέρνηση αποτελείται από διαδικασίες που σχετίζονται όχι μόνο με το εξωτερικό, αλλά και με το εσωτερικό περιβάλλον της Δημόσια Διοίκησης. Προκειμένου να επιτευχθεί η πλήρης δυναμική της, είναι αναγκαίος ο ανασχεδιασμός των διαδικασιών, αφού ληφθούν υπ' όψιν απαιτήσεις και προοπτικές για όλους τους τομείς που περιλαμβάνει. Οι βασικότεροι τομείς (*Domains*) ενός περιβάλλοντος Ηλεκτρονικής Διακυβέρνησης προκύπτουν από την αναγνώριση των εμπλεκόμενων μελών (*Actors*) στις αλληλεπιδράσεις με τη Δημόσια Διοίκηση. Οι πιο συνήθεις εμπλεκόμενοι είναι i) οι πολίτες, ii) οι επιχειρήσεις και iii) η ίδια η Δημόσια Διοίκηση. Βάσει αυτών των εμπλεκομένων προκύπτουν οι ακόλουθοι τομείς:

- *Government to Citizen (G2C)*: περιλαμβάνει όλες τις αλληλεπιδράσεις μεταξύ μεμονωμένων πολιτών και της Δημόσιας Διοίκησης. (π.χ. ηλεκτρονική υποβολή φορολογίας εισοδήματος φυσικών προσώπων)
- *Government to Business (G2B)*: περιλαμβάνει όλες τις αλληλεπιδράσεις μεταξύ επιχειρήσεων και οργανισμών του ιδιωτικού τομέα και της Δημόσιας Διοίκησης. (π.χ. ηλεκτρονική προμήθεια για δημόσιους φορείς)
- *Government to Government (G2G)*: περιλαμβάνει όλες τις αλληλεπιδράσεις μεταξύ φορέων και οργανισμών που εμπίπτουν στη δικαιοδοσία της Δημόσιας Διοίκησης (π.χ. ηλεκτρονική ανταλλαγή πληροφοριών φορέων του Δημοσίου)

Οι τομείς του G2B και G2C χαρακτηρίζονται ως "Εξωτερικό Περιβάλλον Ηλεκτρονικής Διακυβέρνησης" (*external e-Government*) ενώ ο τομέας G2G χαρακτηρίζεται ως "Εσωτερικό Περιβάλλον Ηλεκτρονικής Διακυβέρνησης" (*internal e-Government*). Σε αρκετές περιπτώσεις πραγματοποιείται και ένας επιπλέον διαχωρισμός στο εσωτερικό περιβάλλον, προκειμένου να περιγραφούν οι αλληλεπιδράσεις της Δημόσιας Διοίκησης με Δημόσιους Φορείς άλλων κρατών. Στο Σχήμα 2-1 που ακολουθεί, απεικονίζονται οι τομείς αυτοί.



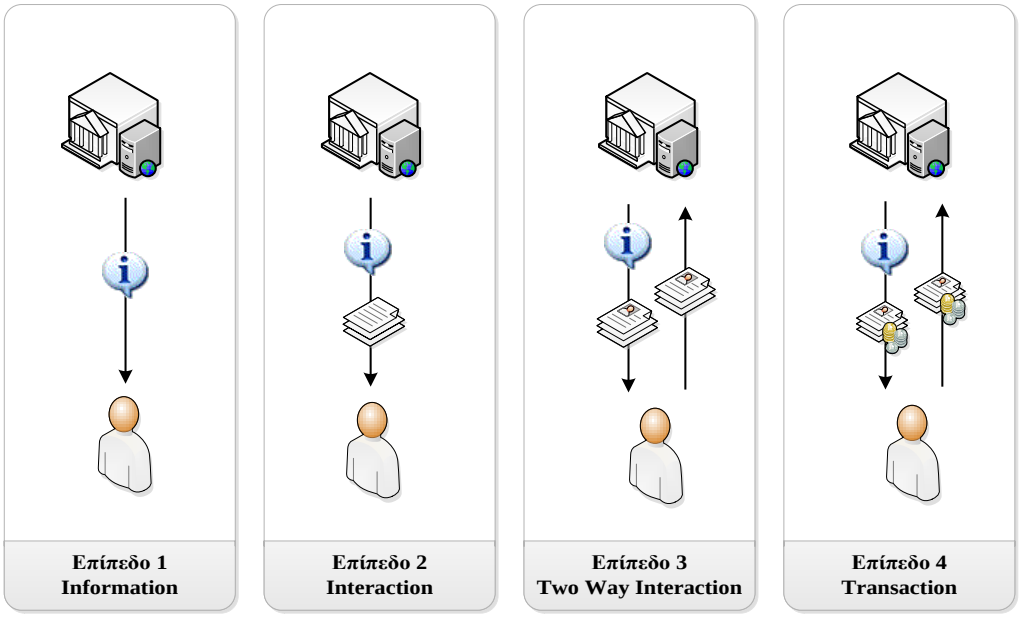
Σχήμα 2-1: Τομείς Ηλεκτρονικής Διακυβέρνησης

2.1.5 Επίπεδα Ολοκλήρωσης Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Οι ηλεκτρονικές υπηρεσίες κατατάσσονται, γενικά, στις ακόλουθες κατηγορίες-επίπεδα, ανάλογα με το βαθμό ολοκλήρωσης (*Online Sophistication*) της υπηρεσίας που μπορεί να επιτευχθεί ηλεκτρονικά:

- *Επίπεδο 1: Πληροφοριακές Υπηρεσίες (Information):* Παροχή πληροφοριακού υλικού σχετικά με τον τρόπο διεκπεραίωσης της υπηρεσίας. Το υλικό αυτό αφορά: στα δικαιολογητικά που πρέπει να προσκομιστούν, στους φορείς που εμπλέκονται για την ολοκλήρωση της υπηρεσίας, στη διαδοχή εκτέλεσης των συναλλαγών που περιλαμβάνει η υπηρεσία, κλπ.
- *Επίπεδο 2: Επικοινωνιακές Υπηρεσίες (Interaction):* Παροχή πληροφοριακού υλικού για τον τρόπο διεκπεραίωσης της υπηρεσίας, καθώς και επίσημο υλικό (πρότυπα αιτήσεων, βεβαιώσεων, κλπ), το οποίο οι χρήστες μπορούν να εξασφαλίσουν με αξιοποίηση του Διαδικτύου, να το εκτυπώσουν και να το χρησιμοποιήσουν κατά τη συναλλαγή τους με το φορέα σε φυσικό επίπεδο.
- *Επίπεδο 3: Διαδραστικές Υπηρεσίες (Two-way interaction):* Πέραν του πληροφοριακού υλικού που παρέχεται σε αυτό το επίπεδο, προσφέρονται on-line φόρμες για συμπλήρωση και ηλεκτρονική αποστολή στην αρμόδια υπηρεσία-φορέα.
- *Επίπεδο 4: Συναλλακτικές Υπηρεσίες (Transactions):* Επιπλέον των φορμών αποστολής στοιχείων, οι ηλεκτρονικές υπηρεσίες που εντάσσονται σε αυτό το επίπεδο υποστηρίζουν λειτουργίες, όπου ο χρήστης ολοκληρώνει τις συναλλαγές που περιλαμβάνει η υπηρεσία. Το γεγονός ότι μία ηλεκτρονική υπηρεσία παρέχει τη δυνατότητα ολοκλήρωσης οικονομικών συναλλαγών, συνεπάγεται τη δυνατότητα πλήρους υποκατάστασης της αντίστοιχης μη-ηλεκτρονικής υπηρεσίας.

Στο Σχήμα 2-2 που ακολουθεί απεικονίζονται τα προαναφερθέντα επίπεδα.



Σχήμα 2-2: Επίπεδα Ολοκλήρωσης Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Από το 2007 και έπειτα, έχει υιοθετηθεί και ένα 5^{ο} επίπεδο ολοκλήρωσης, το οποίο αφορά στην προληπτική και στοχευμένη παροχή υπηρεσιών (*Pro-active Personalization*) (Gapgemini, 2007). Το συγκεκριμένο επίπεδο περιλαμβάνει την αυτοματοποιημένη παροχή ηλεκτρονικών υπηρεσιών, κατά την οποία ο δημόσιος φορέας προβαίνει προληπτικά σε δράσεις με στόχο να βελτιώσει την ποιότητα της παρεχόμενης υπηρεσίας και το βαθμό φιλικότητάς της προς το χρήστη. Επιπρόσθετα, περιλαμβάνει και την αυτόματη εκτέλεση συγκεκριμένων ηλεκτρονικών υπηρεσιών, απαλλάσσοντας από τις αντίστοιχες ενέργειες τον πολίτη ή την επιχείρηση. Το 5ο στάδιο ψηφιακής ολοκλήρωσης μιας υπηρεσίας υφίσταται μόνον για ορισμένες ηλεκτρονικές υπηρεσίες και εκφράζει τις ακόλουθες δύο διαστάσεις:

- Την προληπτική παροχή υπηρεσιών *(proactive automated service delivery)*, όπου η Δημόσια Διοίκηση προχωρά προληπτικά σε δράσεις για να αναβαθμίσει την παροχή μιας ηλεκτρονικής υπηρεσίας και τη φιλικότητά της προς το χρήστη. Παραδείγματα τέτοιων δράσεων αποτελούν η έγκαιρη ειδοποίηση του πολίτη / χρήστη σε περίπτωση που πρέπει να προβεί σε κάποια ενέργεια, η προ- συμπλήρωση δεδομένων σε αιτήσεις του χρήστη προς το Δημόσιο, κ.α.
- Την αυτοματοποιημένη παροχή υπηρεσιών *(automated service provision)*, όπου η Δημόσια Διοίκηση παρέχει αυτόματα συγκεκριμένες υπηρεσίες χωρίς να απαιτείται αντίστοιχη αίτηση από τον πολίτη ή τις επιχειρήσεις..

2.2 Διαλειτουργικότητα σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης

Η έννοια της διαλειτουργικότητας (*Interoperability*) αφορά στα Πληροφοριακά Συστήματα που αξιοποιούνται για την ολοκλήρωση διαδικασιών της Δημόσιας Διοίκησης, και συνδέεται άμεσα με την Ηλεκτρονική Διακυβέρνηση, επιτρέποντας τη μεταφορά και χρήση πληροφορίας με ενιαίο και αποτελεσματικό τρόπο από και προς διαφορετικά Πληροφοριακά Συστήματα. Η διαλειτουργικότητα σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης διακρίνεται σε οργανωσιακή, σημασιολογική και τεχνική, ανάλογα με το αντικείμενο στο οποίο αναφέρεται (ΚΤΠ, 2008):

- *Οργανωσιακή διαλειτουργικότητα (Organisational Interoperability)*: σχετίζεται με τον καθορισμό κοινών στόχων, τη διαμόρφωση διαδικασιών και στην δημιουργία διαύλων συνεργασίας μεταξύ των τμημάτων της Δημόσιας Διοίκησης, με διαφορετικές δομές και διαδικασίες, που επιζητούν την αμοιβαία ανταλλαγή πληροφορίας
- *Σημασιολογική διαλειτουργικότητα (Semantic Interoperability)*: σχετίζεται με τον ορισμό μιας σαφώς προσδιορισμένης και κοινά αποδεκτής περιγραφής της ανταλλασσόμενης πληροφορίας ώστε να είναι κατανοητή και αξιοποιήσιμη από οποιαδήποτε εφαρμογή. Μέσω της δημιουργίας προτύπων διασφαλίζεται κοινή ορολογία και λεξιλόγιο, επιτρέποντας στα Π.Σ. να συνδυάζουν και να επεξεργάζονται πληροφορίες από άλλα Π.Σ.
- *Τεχνική διαλειτουργικότητα (Technical Interoperability)*: σχετίζεται με τη μεταφορά και αξιοποίηση της πληροφορίας σε πραγματικό χρόνο μέσω κατάλληλων φυσικών *(Physical)* και δικτυακών *(Network)* διασυνδέσεων.

2.2.1 Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας

Στο πλαίσιο υποστήριξης της στρατηγικής της Ευρωπαϊκής Ένωσης, έχει θεσπιστεί το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας (*European Interoperability Framework, EIF*) (EC, 2010), με στόχο την παροχή φιλικών, προς τον πολίτη, υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, διασφαλίζοντας παράλληλα τη διαλειτουργικότητα των συστημάτων και των υπηρεσιών σε πανευρωπαϊκό επίπεδο. Οι βασικές αρχές που διέπουν το Ευρωπαϊκό Πλαίσιο είναι:

- *Επικουρικότητα (Subsidiarity) και Αναλογικότητα (Proportionality)*: Όλες οι αποφάσεις θα πρέπει να λαμβάνονται με επίκεντρο το συμφέρον του πολίτη,

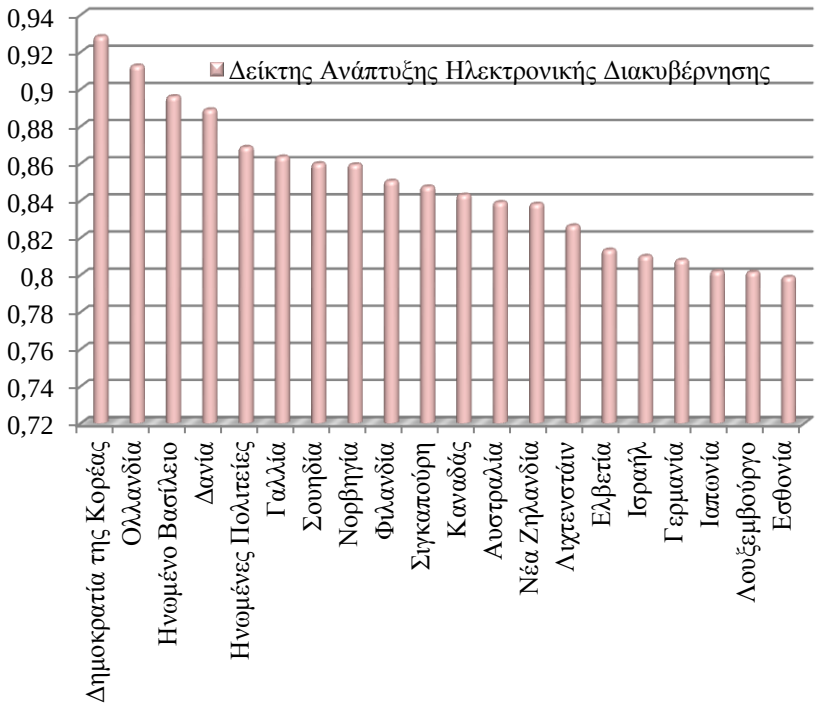
και μόνο εάν είναι πιο αποτελεσματικές από αυτές που ισχύουν σε εθνικό, περιφερειακό ή τοπικό επίπεδο. Επιπρόσθετα, θα παρέχουν τη μεγαλύτερη δυνατή ελευθερία στα Κράτη-Μέλη.

- *Επικέντρωση στο χρήστη (User Centric)*: Οι παρεχόμενες ηλεκτρονικές υπηρεσίες προορίζονται για την εξυπηρέτηση των αναγκών των πολιτών και των επιχειρήσεων και με βάση τις ανάγκες τους θα πρέπει να προσδιοριστεί ποιες υπηρεσίες θα παρέχονται στους πολίτες και με ποιο τρόπο.
- *Ένταξη (Inclusion) και Προσβασιμότητα (Accessibility)*: Οι παρεχόμενες ηλεκτρονικές υπηρεσίες θα πρέπει να είναι προσβάσιμες και προσπελάσιμες από όλες τις κοινωνικές ομάδες, χωρίς αποκλεισμούς σε μειονότητες ή άτομα με ειδικές ανάγκες.
- *Ασφάλεια (Security) και Ιδιωτικότητα (Privacy)*: Όλες οι οντότητες που αλληλεπιδρούν με τη Δημόσια Διοίκηση θα πρέπει να είναι σίγουρες για την ύπαρξη ενός επιπέδου εμπιστοσύνης που συμμορφώνεται πλήρως με τις σχετικές οδηγίες και κανονισμούς.
- *Πολυγλωσσία (Multilingualism)*: Οι παρεχόμενες ηλεκτρονικές υπηρεσίες θα πρέπει να είναι διαθέσιμες σε παραπάνω από μία γλώσσες, χωρίς όμως αυτό να επηρεάζει αρνητικά το επίπεδο των προσφερομένων υπηρεσιών.
- *Διοικητική Απλοποίηση (Administrative simplification)*: Οι Δημόσιοι Φορείς θα πρέπει να συνεργάζονται ώστε να δημιουργήσουν κοινά αξιοποιήσιμες ηλεκτρονικές υπηρεσίες, μειώνοντας και διαμοιράζοντας το φόρτο διαχείρισής τους.
- *Διαφάνεια (Transparency)*: Οι πολίτες και οι επιχειρήσεις θα πρέπει να μπορούν να παρακολουθούν όλες τις διεργασίες της Δημόσιας Διοίκησης, να έχουν εικόνα για το σκεπτικό των αποφάσεων και να μπορούν να ανατροφοδοτήσουν με σχόλια, συμβάλλοντας στη βελτίωση των παρεχόμενων υπηρεσιών.
- *Διατήρηση Πληροφορίας (Preservation of Information)*: Όλες οι διαθέσιμες πληροφορίες και εγγραφές θα πρέπει να διατηρούνται με τέτοιο τρόπο ώστε να εξασφαλίζεται η αναγνωσιμότητα, η αξιοπιστία και η ακεραιότητά τους.
- *Ανοιχτότητα (Openness)*: Όλες οι εμπλεκόμενες οντότητες θα πρέπει να μοιραστούν και να ανταλλάσσουν γνώσεις και πληροφορίες για την αναβάθμιση του επιπέδου των παρεχόμενων υπηρεσιών.

- *Επαναχρησιμοποίηση (Reusability)*: Οι Δημόσιοι Φορείς θα πρέπει να ανταλλάσσουν μεταξύ τους λύσεις, προδιαγραφές και προτυποποιήσεις ώστε να αξιοποιούνται στο έπακρο επιτυχημένες υλοποιήσεις και βέλτιστες πρακτικές.
- *Τεχνολογική Ουδετερότητα (Technological Neutrality) και Προσαρμοστικότητα (Adaptability)*: Ο σχεδιασμός, η υλοποίηση και η παροχή των ηλεκτρονικών υπηρεσιών θα πρέπει να επικεντρώνονται σε πραγματικές λειτουργικές ανάγκες παρά στην επιβολή και αξιοποίηση συγκεκριμένων τεχνολογιών.
- *Αποτελεσματικότητα (Effectiveness) και Αποδοτικότητα (Efficiency)*: Η Δημόσια Διοίκηση θα πρέπει να διασφαλίζει ότι οι παρεχόμενες υπηρεσίες εξυπηρετούν τους πολίτες και τις επιχειρήσεις με τον αποτελεσματικό και αποδοτικό τρόπο.

2.3 Εξέλιξη Ηλεκτρονικής Διακυβέρνησης ανά τον Κόσμο

Η έκθεση των Ηνωμένων Εθνών για το 2012 για την ανάπτυξη της Ηλεκτρονικής Διακυβέρνηση σε παγκόσμιο επίπεδο (United Nations, 2012), επικεντρώνεται στην έννοια των ενοποιημένων - ολοκληρωμένων υπηρεσιών που αξιοποιούν διασυνδέσεις μεταξύ διαφόρων δημόσιων υπηρεσιών και θεματικά παρόμοιων διαδικτυακών πυλών μίας στάσης, που μπορούν να αναμορφώσουν την ηλεκτρονική παροχή δημόσιων υπηρεσιών τόσο στο εμπρόσθιο τμήμα (*Front-end*) όσο και στο οπίσθιο (*Back-end*), να αυξήσουν την λειτουργική παραγωγικότητα, καθώς και τη βελτίωση των διαδικασιών και μηχανισμών διακυβέρνησης σε διάφορους τομείς της Δημόσιας Διοίκησης. Και οι 20 χώρες που σημειώνουν τους υψηλότερους δείκτες ανάπτυξης, συμπεριλαμβάνονται στις υψηλά ανεπτυγμένες οικονομίες. Από αυτές, οι 14 είναι στη Βόρεια Αμερική και την Ευρώπη, 3 στην Ανατολική Ασία (Δημοκρατία της Κορέας, Σιγκαπούρη και Ιαπωνία), 2 στην Ωκεανία (Αυστραλία και Νέα Ζηλανδία και 1 στη Δυτική Ασία (Ισραήλ). Το Σχήμα 2-3, στη συνέχεια, παρουσιάζει τους δείκτες ανάπτυξης για καθεμία από αυτές τις 20 χώρες.

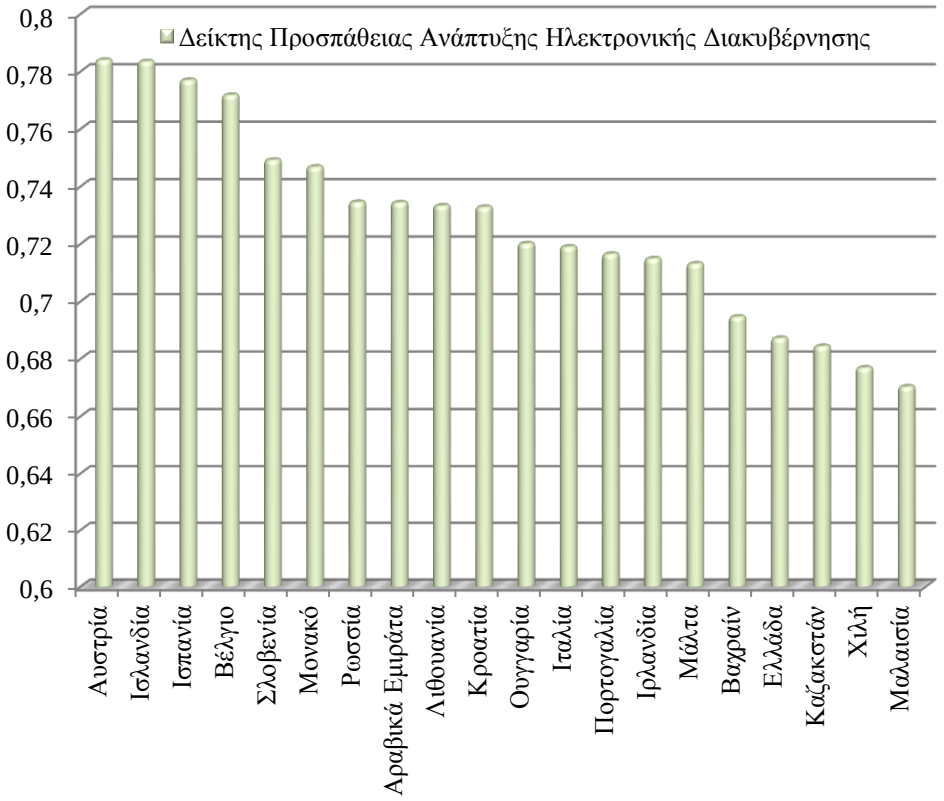


Σχήμα 2-3: Δείκτης Ανάπτυξης Ηλεκτρονικής Διακυβέρνησης σε Παγκόσμιο Επίπεδο (United Nations, 2012)

Η Δημοκρατία της Κορέας είναι ο παγκόσμιος ηγέτης στην ανάπτυξη (0,9283), ακολουθούμενη από την Ολλανδία (0,9125), το Ηνωμένο Βασίλειο (0,8960) και τη Δανία (0.8889), με τις Ηνωμένες Πολιτείες, τον Καναδά, τη Γαλλία, τη Νορβηγία, τη Σιγκαπούρη και Σουηδία να βρίσκονται πιο πίσω. Σε σύγκριση με την αντίστοιχη έκθεση του 2010 (United Nations, 2010) παρατηρείται μία σταθερή βελτίωση των δεικτών ανάπτυξης σε παγκόσμιο επίπεδο, κάτι που οδήγησε στην αύξηση του μέσου όρου από 0,4406 σε 0,4877. Αυτή η αύξηση έρχεται να επιβεβαιώσει την αυξημένη προσπάθεια που παρατηρείται τα τελευταία χρόνια για παροχή υπηρεσιών Ηλεκτρονικής Διακυβέρνησης. Παρόλα αυτά όμως, παραμένει αρκετά μεγάλο το χάσμα που παρατηρείται μεταξύ των οικονομικά ανεπτυγμένων και μη κρατών, ιδιαίτερα στις χώρες της Αφρικής. Αυτή η διαφορά αποδίδεται κατά μεγάλο βαθμό στην έλλειψη τεχνολογικής υποδομής και διάδοσης της ευρυζωνικότητας (*Broadband*).

Αμέσως μετά τις χώρες που κατατάσσονται πρώτες σε παγκόσμιο επίπεδο, βρίσκονται οι λεγόμενοι "αναδυόμενοι ηγέτες", όπως παρουσιάζονται στο Σχήμα 2-4 παρακάτω. Ως τέτοιες χαρακτηρίζονται οι χώρες εκείνες που έχουν σημειώσει σημαντική βελτίωση σε σχέση με προηγούμενες εκθέσεις. Πρώτη σε αυτή την κατάταξη είναι η Αυστρία (0,7840) και ακολουθούν η

Ισλανδία (0,7835), η Ισπανία (0,7770) και το Βέλγιο (0,7718). Σημαντική αύξηση παρατηρείται στους δείκτες της Ρωσίας (0,7345), των Ηνωμένων Αραβικών Εμιράτων (0,7344) και της Σαουδικής Αραβίας (0,6658) καθώς επίσης στην περίπτωση της Ιταλίας (0,7190) και της Πορτογαλίας (0,7165). Τέλος, αξιοσημείωτη είναι και η πρόοδος που σημείωσε η Ελλάδα (0.6872) σε σχέση με τον δείκτη του 2010 (0,5708).



Σχήμα 2-4: Δείκτης Προσπάθειας Ανάπτυξης Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης (United Nations, 2012)

2.4 Η Ηλεκτρονική Διακυβέρνηση στην Ελλάδα

Η προσπάθεια της Ελληνικής Δημόσιας Διοίκησης για την μετάβαση στην Ηλεκτρονική Διακυβέρνηση και την Κοινωνία της Πληροφορίας ξεκίνησε στο 1994 με την υποστήριξη των Κοινοτικών Πλαισίων Στήριξης (ΚΠΣ) (Markellos et al., 2007). Αρχικά οι προσπάθειες αφορούσαν στην ανάπτυξη κυβερνητικών ιστοτόπων για την παροχή πληροφοριακού, κυρίως, υλικού. Το 1999 διαμορφώθηκε η εθνική στρατηγική προσέγγιση στην Ηλεκτρονική Διακυβέρνηση και την

Κοινωνία της Πληροφορίας, με έμφαση στο σχεδιασμό για όλους και στην ποιότητα των παρεχόμενων υπηρεσιών, με απώτερο σκοπό να διασφαλιστεί η κοινωνική συνοχή και η βελτίωση του βιοτικού επιπέδου (Gouscos et al., 2000). Από το 2000 και έπειτα ξεκινά η παροχή ορισμένων υπηρεσιών Ηλεκτρονικής Διακυβέρνησης (Hahamis et al., 2005). Όμως, ο Δημόσιος Τομέας στην Ελλάδα χαρακτηρίζεται από ιδιαίτερη πολυπλοκότητα, χαμηλή απόδοση, έλλειψη μηχανογράφησης και τεχνολογικών υποδομών καθώς και από μικρό ποσοστό δαπανών για ΤΠΕ, χαρακτηριστικά τα οποία καθιστούν δύσκολη την εφαρμογή της ΗΔ (Κιοσσέ, 2011).

2.4.1 Νομικό και Κανονιστικό Πλαίσιο

Στην κατεύθυνση ορισμού ενός ολοκληρωμένου θεσμικού πλαισίου για την επικοινωνία, με ηλεκτρονικά μέσα, με φορείς του Δημόσιου Τομέα, διακρίνονται οι παρακάτω κανονιστικές πράξεις:

- Άρθρο 5Α του Συντάγματος: Κατοχυρώνει το δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας βρίσκοντας αντίκρισμα στην ηλεκτρονική επικοινωνία Δημόσιας Διοίκησης και πολίτη, την πρόσβαση σε δημόσια πληροφορία και υπηρεσίες Ηλεκτρονικής Διακυβέρνησης.
- Άρθρο 9Α του Συντάγματος: Κατοχυρώνεται η προστασία του ατόμου από συλλογή, επεξεργασία και χρήση προσωπικών δεδομένων, καθώς και η ιδιωτικότητα του υποκειμένου των πληροφοριών, σταθμίζοντας το δικαίωμα συμμετοχής σε περιβάλλοντα με απεριόριστες δυνατότητες πρόσβασης σε πληροφορία.

Ο Ν. 3979/2011 (ΦΕΚ Α’ 138) ορίζει το θεσμικό πλαίσιο για την εφαρμογή και την προώθηση της ηλεκτρονικής διακυβέρνησης σε όλο το εύρος του δημόσιου τομέα, με το οποίο οργανώνεται και απλοποιείται η σχέση της Δημόσιας Διοίκησης με τους πολίτες και τις επιχειρήσεις, αξιοποιώντας τις ΤΠΕ. Ο νόμος προδιαγράφει τις προϋποθέσεις για την υλοποίηση ενός πλαισίου παροχής ηλεκτρονικών υπηρεσιών με εμπλεκόμενα μέρη τους φορείς της Δημόσιας Διοίκησης, τους πολίτες και τις επιχειρήσεις. Με γνώμονα την εξυπηρέτηση και διευκόλυνση των φυσικών και νομικών προσώπων μέσα από την απλούστευση διαδικασιών, την δραστική μείωση των διοικητικών επιβαρύνσεων, γραφειοκρατικών φαινομένων καθώς και την εδραίωση σχέσεων

εμπιστοσύνης, ο νόμος στοχεύει σε ποιοτικότερες, ασφαλέστερες ταχύτερες και πιο ευέλικτες υπηρεσίες. Πιο συγκεκριμένα εισάγει πλήθος καινοτομιών, όπως είναι:

- Η έκδοση ηλεκτρονικών διοικητικών πράξεων με παράλληλη κατοχύρωση των προϋποθέσεων για τη νομική και αποδεικτική ισχύ των ηλεκτρονικών εγγράφων,
- Η αυτεπάγγελτη ή κατ' αίτηση αναζήτηση εγγράφων που τηρούνται σε οποιοδήποτε φορέα του Δημόσιου Τομέα, απαλλάσσοντας τον πολίτη και τις επιχειρήσεις από διαδικασίες επικύρωσης αντιγράφων για τις συναλλαγές τους με τη Δημόσια Διοίκηση και
- Η καθιέρωση της δυνατότητας ηλεκτρονικών συναλλαγών, συμπεριλαμβανομένων και των ηλεκτρονικών οικονομικών συναλλαγών και πληρωμών με φορείς του Δημόσιου Τομέα.

Ιδιαίτερη έμφαση δίνεται στους ακόλουθους τομείς:

- Στην ηλεκτρονική επικοινωνία και ανταλλαγή δεδομένων μεταξύ προσώπων (φυσικών και νομικών) και δημόσιων φορέων, τόσο με τη διάσταση της ενδοδιοικητικής επικοινωνίας, διακίνησης εγγράφων και διεκπεραίωσης διοικητικών πράξεων, όσο και με την παραγωγή ηλεκτρονικών διοικητικών πράξεων και εγγράφων. Δημιουργείται έτσι το θεσμικό πλαίσιο για την παροχή ηλεκτρονικών υπηρεσιών από τη Δημόσια Διοίκηση, την ηλεκτρονική διακίνηση εγγράφων και το ηλεκτρονικό πρωτόκολλο.
- Στη νομική και αποδεικτική ισχύ ηλεκτρονικά παραγόμενων και διακινούμενων εγγράφων, όπου εξασφαλίζεται η εξίσωση της νομικής και αποδεικτικής ισχύος των ηλεκτρονικών εγγράφων που φέρουν προηγμένη ψηφιακή υπογραφή εξουσιοδοτημένου οργάνου, βασισμένη σε αναγνωρισμένο ψηφιακό πιστοποιητικό με έγγραφα που φέρουν ιδιόχειρη υπογραφή και σφραγίδα.
- Στην πληροφορία που διατίθεται δημόσια από Δημόσιους Φορείς , στον τρόπο που αυτή πρέπει να γίνεται αντικείμενο επεξεργασίας, προκειμένου να καθίσταται χρήσιμη και αξιοποιήσιμη, και σε θέματα ανοικτής πρόσβασης σε δημόσια δεδομένα.
- Σε θέματα ηλεκτρονικών πληρωμών, όπου, ανεξάρτητα από την ιδιότητα του συναλλασσομένου (δικαιούχος ή οφειλέτης) και σύμφωνα με προϋποθέσεις

ταυτοποίησης και επιβεβαίωσης της ταυτότητάς του, η διεκπεραίωση τέτοιων πράξεων μπορεί να πραγματοποιηθεί απευθείας από τον ίδιο.

- Σε ζητήματα προστασίας προσωπικών δεδομένων και προστασίας της ιδιωτικότητας του πολίτη. Προς αυτή την κατεύθυνση εισάγεται η αξιολόγηση των επιπτώσεων (*Privacy Impact Assessment*) και των κινδύνων (*Risks*) που σχετίζονται με την προάσπιση της ιδιωτικότητας και την προστασία δεδομένων προσωπικού χαρακτήρα κατά τον σχεδιασμό, διαμόρφωση και προμήθεια Π.Σ. και υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, με ταυτόχρονη μέριμνα για την όσο το δυνατόν ελάχιστη επεξεργασία δεδομένων προσωπικού χαρακτήρα, λαμβάνοντας υπόψη τη -συνταγματική και νομοθετική- επιταγή για προστασία τους κατά το σχεδιασμό (*Privacy by Design*). Ειδικότερα, ορίζει ότι τα πρόσωπα μπορούν να επιλέξουν την επαναχρησιμοποίηση των προσωπικών δεδομένων που έχουν γνωστοποιήσει σε φορείς του Δημόσιου Τομέα, για μελλοντικές συναλλαγές, ηλεκτρονικές ή μη, υπό την προϋπόθεση της ενημερωμένης συγκατάθεσής τους (*Informed Consent*).

Τέλος, πέραν του Ν. 3979 / 2011, διακρίνονται και οι παρακάτω ρυθμιστικός - κανονιστικές πράξεις:

- Άρθρο 14, Ν. 2672/1998 «Διακίνηση Εγγράφων με Ηλεκτρονικά Μέσα»: Προσδιορίζεται η δυνατότητα ηλεκτρονικής επικοινωνίας με φορείς της Δημόσιας Διοίκησης, μέσω τηλεομοιοτυπίας (*Fax*) και ηλεκτρονικού ταχυδρομείου.
- Π.Δ. 342/2002: Ρυθμίζει τη διακίνηση εγγράφων μέσω ηλεκτρονικού ταχυδρομείου μεταξύ υπηρεσιών και φορέων της Δημόσιας Διοίκησης ή μεταξύ φυσικών και νομικών προσώπων ιδιωτικού δικαίου.
- Άρθρο 8, Ν. 3242/2004: Θεσμοθετεί τη δυνατότητας διεκπεραίωσης διοικητικών συναλλαγών από την αρμόδια για την έκδοση της τελικής πράξης υπηρεσία με τη χρήση ηλεκτρονικών μέσων.

2.4.2 Εξέλιξη Είκοσι Βασικών Δημόσιων Ηλεκτρονικών Υπηρεσιών

Το Μάιο του 2013 δημοσιεύθηκαν τα αποτελέσματα της έρευνας του Παρατηρητηρίου για τη Διοικητική Μεταρρύθμιση της Κοινωνίας της Πληροφορίας, όπου αποτυπώνεται η εξέλιξη

20 βασικών υπηρεσιών Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα (Παρατηρητήριο για τη Διοικητική Μεταρρύθμιση, 2013). Πρόκειται για 20 ηλεκτρονικές υπηρεσίες, που αξιολογούνται σε ευρωπαϊκό επίπεδο βάσει κοινής μεθοδολογίας για λόγους συγκριτικής αξιολόγησης μεταξύ των κρατών – μελών, από τις οποίες οι 12 αφορούν τους πολίτες και οι υπόλοιπες 8 τις επιχειρήσεις.

	Α/Α	**Βασικές Δημόσιες Υπηρεσίες**	**Επίπεδο Ολοκλήρωσης**	**Δημόσιος Φορέας Πάροχος Υπηρεσίας**
Ηλεκτρονικές Υπηρεσίες προς Πολίτες	1	Φόρος εισοδήματος: δήλωση και ειδοποίηση εκκαθάρισης	5	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	2	Υπηρεσίες Αναζήτησης Εργασίας	4	Οργανισμός Απασχόλησης Εργατικού Δυναμικού (ΟΑΕΔ)
	3	Εισφορές Κοινωνικής Ασφάλισης	2,25[2]	Οργανισμός Απασχόλησης Εργατικού Δυναμικού (ΟΑΕΔ)
	4	Προσωπικά έγγραφα (διαβατήριο και άδεια οδήγησης)	2,5	Υπουργείο Δημοσίας Τάξης & Προστασίας του Πολίτη - Ελληνική Αστυνομία (διεύθυνση διαβατηρίων)/ Κέντρα Ενημέρωσης Πολιτών (ΚΕΠ)
	5	Καταχώρηση Οχήματος	n/a**[3]	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	6	Έκδοση Οικονομικής Άδειας	2	e- ΠΟΛΕΟΔΟΜΙΑ (Υπουργείο Περιβάλλοντος Ενέργειας & Κλιματικής Αλλαγής (ΥΠΕΚΑ) & Υπουργείο Εσωτερικών (ΥΠΕΣ))
	7	Δήλωση προς την Αστυνομία (π.χ., σε περίπτωση κλοπής)	1	Υπουργείο Δημοσίας Τάξης & Προστασίας του Πολίτη – Ελληνική Αστυνομία
	8	Δημόσιες βιβλιοθήκες (διαθεσιμότητα καταλόγων, εργαλεία αναζήτησης)	4	Υπουργείο Παιδείας & Θρησκευμάτων, Πολιτισμού & Αθλητισμού

[2] Στις Εισφορές Κοινωνικής Ασφάλισης και Προσωπικά Έγγραφα περιλαμβάνονται επιμέρους υπηρεσίες με διαφορετικό επίπεδο ολοκλήρωσης. Σαν συνολική επίδοση υπολογίζεται ο μέσος όρος των επιμέρους επιδόσεων.

[3] Η υπηρεσίες «Δήλωση Αυτοκινήτου», παρέχονταν μέχρι πρόσφατα από τη Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ) αλλά πλέον είναι εκτός λειτουργίας. Τα στοιχεία όμως χρησιμοποιούνται για την έκδοση των τελών κυκλοφορίας.

	Α/Α	Βασικές Δημόσιες Υπηρεσίες	Επίπεδο Ολοκλήρωσης	Δημόσιος Φορέας Πάροχος Υπηρεσίας
	9	Πιστοποιητικά (Γεννήσεως και Γάμου): αίτηση & παραλαβή	3	Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ)
	10	Εισαγωγή στην Ανώτατη Εκπαίδευση	2	Υπουργείο Παιδείας & Θρησκευμάτων, Πολιτισμού & Αθλητισμού
	11	Ανακοίνωση Μετακόμισης – Αλλαγή Διεύθυνσης	4	Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ)
	12	Υπηρεσίες Υγείας (διαθεσιμότητα υπηρεσιών & κλείσιμο ραντεβού)	2	Υπουργείο Υγείας
Ηλεκτρονικές Υπηρεσίες προς Επιχειρήσεις	13	Εισφορές Κοινωνικής Ασφάλισης για Εργαζομένους	4	Ίδρυμα Κοινωνικών Ασφαλίσεων (ΙΚΑ)
	14	Φόρος Επιχειρήσεων: Δήλωση & Ειδοποίηση Εκκαθάρισης	4	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	15	ΦΠΑ: Δήλωση & Ειδοποίηση Εκκαθάρισης	4	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	16	Έναρξη Επιχείρησης	2	Γενική Γραμματεία Εμπορίου (ΓΓΕ)
	17	Υποβολή Στοιχείων σε Στατιστικές Υπηρεσίες	4	Ελληνική Στατιστική Αρχή (ΕΛ.ΣΤΑΤ.)
	18	Δηλώσεις στα Τελωνεία	4	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	19	Περιβαλλοντικές Άδειες	2	Υπουργείο Περιβάλλοντος, Ενέργειας & Κλιματικής Αλλαγής/ Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ)
	20	Δημόσιες Προμήθειες	2	Γενική Γραμματεία Εμπορίου (ΓΓΕ)

Πίνακας 2-2: Βασικές Δημόσιες Ηλεκτρονικές Υπηρεσίες (Παρατηρητήριο για τη Διοικητική Μεταρρύθμιση, 2013)

2.4.3 Εθνική Στρατηγική για την Ηλεκτρονική Διακυβέρνηση

Η πιο πρόσφατη Εθνική Στρατηγική για την Ηλεκτρονική Διακυβέρνηση (Επιτροπή Συντονισμού της Ηλεκτρονικής Διακυβέρνησης, 2013), όπως δημοσιεύτηκε το Μάιο του 2013, έχει ως στόχο να καθορίσει με σαφήνεια ένα νέο τομέα ανάπτυξης της χώρας, σε συνδυασμό πάντα με τον αντίστοιχο στρατηγικό σχεδιασμό για τις ΤΠΕ στην Ελλάδα τα επόμενα δέκα χρόνια,

και σε συνεργασία με τα συναρμόδια Υπουργεία, βασισμένη στις αρχές της ανταγωνιστικότητας, της παραγωγικότητας, της εξωστρέφειας, την επενδυτική ενίσχυση και φυσικά την ανάπτυξη της απασχόλησης. Οι κύριοι στόχοι της Στρατηγικής συνοψίζονται στα ακόλουθα σημεία:

- Παροχή του μέγιστου δυνατού αριθμού ψηφιακών υπηρεσιών προς τον πολίτη και την επιχείρηση ειδικότερα υπηρεσιών "4ου ή 5ου επιπέδου", δηλαδή υπηρεσιών που ολοκληρώνονται διαδικτυακά, χωρίς φυσική παρουσία του πολίτη στη Δημόσια Διοίκηση.
- Δημιουργία περιβάλλοντος πλήρους ψηφιακής συνεργασίας/επικοινωνίας μεταξύ των υπηρεσιών και των στελεχών της δημόσιας διοίκησης
- Χρήση σύγχρονων υποδομών και διασφάλιση ποιοτικών και ασφαλών συνθηκών ψηφιακής ανάπτυξης για τους πολίτες, τις επιχειρήσεις και τον δημόσιο τομέα.

Η προσπάθεια για επίτευξη των παραπάνω στόχων γίνεται με κανόνες διασφάλισης του απαραβίαστου των ευαίσθητων προσωπικών δεδομένων και σεβασμό στη σφαίρα της ιδιωτικής ζωής των πολιτών.

ΚΕΦΑΛΑΙΟ 3 - ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Στο παρόν κεφάλαιο εξετάζεται η έννοια της Ιδιωτικότητας Πληροφοριών, η ανάγκη προάσπισής της σε Πληροφορικά Συστήματα Ηλεκτρονικής Διακυβέρνησης, καθώς και το νομικό και κανονιστικό πλαίσιο σε Ευρωπαϊκό και Εθνικό επίπεδο. Στη συνέχεια καταγράφονται και επισκοπούνται ολοκληρωμένα, ύστερα από πρωτογενή και δευτερογενή έρευνα, οι βασικές παράμετροι για την ανάλυση - αποτίμηση της επικινδυνότητας (*Risk Assessment*), μέσω της ανάλυσης τόσο των δυνητικών απειλών (*Threats*) που υφίστανται οι συναλλαγές των πολιτών και των επιχειρήσεων σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης, όσο και των αρνητικών επιπτώσεων (*Impact*) που μπορούν να προκληθούν στον πάροχο της υπηρεσίας ή και στον τελικό χρήστη.

3.1 Η Έννοια της Ιδιωτικότητας

Η πρώτη νεότερη αναφορά στην ανάγκη να επισημανθεί η αξία της ιδιωτικότητας εντοπίζεται το 1890 (Brandeis & Warre, 1980) όπου για πρώτη φορά η ιδιωτικότητα συνδέεται με "*το δικαίωμα να μείνει κανείς μόνος του*" ("*the right to be left alone*") και επισημαίνεται η αναγκαιότητα να κατοχυρωθεί συνταγματικά ως έννοια. Το 1948, το Γενικό Συμβούλιο των Ηνωμένων Εθνών στην "Παγκόσμια Δήλωση των Ανθρωπίνων Δικαιωμάτων"s αναφέρεται γενικά στο θέμα της ιδιωτικότητας και το 1950 η Ευρωπαϊκή Επιτροπή των Ανθρωπίνων Δικαιωμάτων θεσπίζει το δικαίωμα σεβασμού της ιδιωτικής ζωής των πολιτών της. Η έννοια της ιδιωτικότητας, ανάλογα το είδος και πλαίσιο (*Context*) των πληροφοριών, μπορεί να διαχωριστεί στις κάτωθι εκφάνσεις (Rosenberg, 1992) :

- *Ιδιωτικότητα Πληροφοριών (Informational Privacy)*: αφορά στον έλεγχο του αν και πώς τα προσωπικά δεδομένα ενός προσώπου μπορούν να συγκεντρωθούν, να αποθηκευτούν, να υποστούν επεξεργασία ή να διαδοθούν επιλεκτικά.
- *Εδαφική (Μη προσπελασιμότητα του Χώρου) Ιδιωτικότητα (Territorial Privacy)*: αφορά στην προστασία της στενής φυσικής περιοχής που περιβάλλει ένα πρόσωπο, δηλαδή οικιακά και άλλα περιβάλλοντα, όπως ο εργασιακός ή ο δημόσιος χώρος.

- *Σωματική Ιδιωτικότητα (Bodily Privacy)*: αφορά στην προστασία ενός προσώπου από αδικαιολόγητη παρέμβαση, όπως ο σωματικός έλεγχος, η υποχρεωτική υποβολή σε εξέταση/επέμβαση, η δοκιμή φαρμάκων, πληροφορίες που παραβιάζουν την ηθική αίσθηση του ατόμου.
- *Ιδιωτικότητα Επικοινωνίας (Communication Privacy)*: αφορά στην προστασία της επικοινωνίας ενός προσώπου από μη εξουσιοδοτημένη παρακολούθηση.

Αξίζει να σημειωθεί ότι έκτοτε έχουν προταθεί αρκετές κατηγοριοποιήσεις - διαχωρισμοί της έννοιας της ιδιωτικότητας ανάλογα και με πλαίσιο των πληροφοριών (Clarke, 1997), (Massey & Antón, 2008), (Barker et al., 2009), (Solove, 2009).

Τα δεδομένα (*Data*) αναδείχθηκαν, σημασιοδοτήθηκαν και καθιερώθηκαν ως "ξεχωριστός" όρος σε συνάρτηση με την επεξεργασία δεδομένων και κυρίως με την ανάπτυξη και διάδοση της αυτοματοποιημένης επεξεργασίας δεδομένων. Η συσχέτιση αυτή αναπόφευκτα τονίζει το "δεδομένο" ως τεχνικό όρο και μέρος ενός συστήματος επεξεργασίας, και οδηγεί στον προσδιορισμό των "δεδομένων" ως στοιχείων μιας "επεξεργασμένης" πληροφορίας, ως στοιχεία της πληροφορίας που έγινε αντικείμενο αυτοματοποιημένης επεξεργασίας. Στην έννοια του δεδομένου προσδίδεται μία ουδετερότητα όσον αφορά στον σκοπό, ενώ η έννοια της πληροφορίας συσχετίζεται με την χρησιμότητά της. Ανεξάρτητα από τις εννοιολογικές διαφορές οι δύο όροι έχουν καταλήξει να είναι συνώνυμοι (Μήτρου, 2006).

Στα περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης, η συζήτηση για την ιδιωτικότητα και κατά συνέπειά για την προάσπισή της περιστρέφεται κυρίως γύρω από την ιδιωτικότητα των πληροφοριών και την ιδιωτικότητα της επικοινωνίας, καθώς δεν επηρεάζεται άμεσα η εδαφική και σωματική ακεραιότητα (Auerbach, 2004). Η επιτυχημένη παροχή υπηρεσιών Ηλεκτρονικής Διακυβέρνησης εξαρτάται σε μεγάλο βαθμό από τη διασφάλιση προάσπισης της ιδιωτικότητας των δεδομένων και πληροφοριών που αξιοποιούνται για την ολοκλήρωσή τους. Τα προσωπικά δεδομένα και πιο συγκεκριμένα η επεξεργασία τους ανάγεται ταυτόχρονα σε κρίσιμο παράγοντα λήψης αποφάσεων στο πλαίσιο της άσκησης κρατικών καθηκόντων και αρμοδιοτήτων και εν γένει της δραστηριότητας του Δημόσιου τομέα, (Μήτρου, 2002) (Μήτρου, 2006) Οι απειλές που ανακύπτουν είναι είτε εγγενείς, αφορούν δηλαδή στη χρήση του Διαδικτύου ως μέσου επικοινωνίας, είτε αφορούν σε συγκεκριμένα ειδικά ζητήματα, όπως είναι η χρήση αναγνωριστικών χρηστών και η διασύνδεση δεδομένων και πληροφοριών (Ιγγλεζάκης, 2007).

3.1.1 Ιδιωτικότητα Πληροφοριών σε Περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης

Ο πιο κοινά αποδεκτός ορισμός της ιδιωτικότητας των πληροφοριών προτάθηκε το 1967 (Westin, 1967) και αναφέρει «*Η ιδιωτικότητα είναι η αξίωση των ατόμων, των ομάδων και των ιδρυμάτων, να αποφασίζουν από μόνοι τους για το πότε, πώς και μέχρι ποιο σημείο οι πληροφορίες που αφορούν αυτούς, θα διαβιβάζονται σε άλλους*". Το σημαντικότερο σημείο της έννοιας της Ιδιωτικότητας Πληροφοριών αποτελεί ο διαχωρισμός των πληροφοριών που είναι δημόσια διαθέσιμες και αυτών που χαρακτηρίζονται ως ιδιωτικές και πρέπει να προστατευτούν. Ο προσδιορισμός της κατηγορίας στην οποία εντάσσεται κάθε είδος πληροφορίας, εξαρτάται από διάφορους παράγοντες και συνήθως βασίζεται στο ισχύον νομικό και κανονιστικό πλαίσιο. Μάλιστα, η ευρεία εξάπλωση των Π.Σ έχει αναδείξει και το δικαίωμα της ηθελημένης αυτοδιάθεσης πληροφοριών που θα μπορούσαν να χαρακτηριστούν και ως ιδιωτικές, καθώς το υποκείμενό τους συνεχίζει να έχει την επιλογή διάθεσής τους για συγκεκριμένο σκοπό και χρήση .

Η έννοια της Ιδιωτικότητας των Πληροφοριών καθίσταται εξαιρετικά σημαντική σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης, εξαιτίας τόσο του χαρακτήρα των πληροφοριών που αξιοποιούνται όσο και του σημαντικού όγκου που συλλέγεται, επεξεργάζεται και αποθηκεύεται (Vrakas et al., 2010). Παραδείγματα τέτοιων πληροφοριών – δεδομένων αποτελούν τα διάφορα αναγνωριστικά (τομεακά ή μη) που αξιοποιεί ο κάθε χρήστης: οικονομικά – φορολογικά στοιχεία, δημογραφικά στοιχεία, ποινικό μητρώο, ιατρικά αρχεία και δεδομένα που σχετίζονται με θρησκευτικές και πολιτικές πεποιθήσεις. Επιπρόσθετα, η ιδιαιτερότητα των υπηρεσιών που προσφέρονται από τη Δημόσια Διοίκηση έγκειται στην υποχρέωση παροχής όλων των απαιτούμενων πληροφοριών – δεδομένων, σε αντίθεση με τις ηλεκτρονικές υπηρεσίες σε Π.Σ. ηλεκτρονικού εμπορίου ή ηλεκτρονικής μάθησης, όπου ο χρήστης μπορεί να επιλέξει να μην παρέχει κάποιες πληροφορίες αλλά παρόλα αυτά να καταστεί δυνατή η παροχή της υπηρεσίας.

3.1.2 Απαιτήσεις Ασφάλειας και Ιδιωτικότητας Δεδομένων

Οι απαιτήσεις ασφάλειας και ιδιωτικότητας των δεδομένων - πληροφοριών που αξιοποιούνται σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης, και προκύπτουν από την ανάγκη προστασίας τους, περιλαμβάνουν τα κάτωθι (Γκρίτζαλης, 2004) (ISO/IEC 27001, 2013):

- *Εμπιστευτικότητα (Confidentiality)*: αφορά στην προστασία από αποκάλυψη δεδομένων σε μη εξουσιοδοτημένες οντότητες,

- *Ακεραιότητα (Integrity)*: αφορά στην προστασία από μη εξουσιοδοτημένη εισαγωγή, τροποποίηση ή διαγραφή δεδομένων,
- *Διαθεσιμότητα (Availability)*: αφορά στην προστασία από μη-διάθεση των δεδομένων,
- *Αυθεντικότητα (Authenticity)*: αφορά στη διασφάλιση της ταυτότητας κάθε εμπλεκόμενης οντότητας,
- *Μη Αποποίηση (Non Repudiation)*: αφορά στην προστασία από άρνηση μια οντότητας για πραγματοποίηση συγκεκριμένης δραστηριότητας.

Για την μετατροπή της ιδιωτικότητας από μία γενική έννοια σε τεχνική απαίτηση έχουν ορισθεί οι επιμέρους απαιτήσεις ιδιωτικότητας (Fischer-Hübner, 2001), (Cannon, 2004) (Καλλονιάτης, 2011) :

- *Αυθεντικοποίηση (Authentication)*: η διαδικασία μέσω της οποίας επιβεβαιώνεται η ταυτότητα μιας οντότητας. Αποτελεί κυρίως απαίτηση ασφάλειας, παρά ιδιωτικότητας ενός Π.Σ., ωστόσο έχει σημαντική συνεισφορά και στην ικανοποίηση απαιτήσεων ιδιωτικότητας.
- *Εξουσιοδότηση (Authorization)*: η διαδικασία μέσω της οποίας μία οντότητα αποκτά δικαιώματα - πρόσβαση σε μια μεμονωμένη υπηρεσία ή σε συγκεκριμένες υπηρεσίες ενός πληροφοριακού συστήματος.
- *Αναγνώριση (Identification)*: η διαδικασία μέσω της οποία ελέγχεται αν η υπηρεσία ή τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση και στη συνέχεια εξουσιοδότησή της ή όχι.
- *Προστασία Δεδομένων (Data Protection)*: η διαδικασία μέσω της οποίας διασφαλίζονται, σύμφωνα και με την Ευρωπαϊκή Οδηγία 1995/46/ΕΚ, οι κάτωθι αρχές:
    - Αρχή της νομιμότητας και της δικαιοσύνης.
    - Αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν.
    - Αρχή της αναγκαιότητας της συλλογής και επεξεργασίας των δεδομένων.
    - Παροχή πληροφόρησης, ενημέρωσης και πρόσβασης στους κατόχους των δεδομένων.

- Αρχή της ασφάλειας και της ακεραιότητας.
- Εποπτεία και Επικύρωση.

- *Ανωνυμία (Anonymity)*: η διαδικασία μέσω της οποίας διασφαλίζεται ότι μία οντότητα μπορεί να χρησιμοποιήσει μια υπηρεσία ή να επικοινωνήσει με μια άλλη οντότητα χωρίς να αποκαλύψει την ταυτότητά του.
- *Ψευδωνυμία (Pseydonymity)*: η διαδικασία μέσω της οποίας προστατεύεται η αναγνώριση (*Identification*) μιας οντότητας από μη εξουσιοδοτημένες τρίτες οντότητες.
- Μη-*συνδεσιμότητα (Unlinkability)*: η διαδικασία μέσω της οποίας προστατεύεται η ιδιωτικότητα μιας οντότητας από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να συνδέσουν τμήματα σχετικών πληροφοριών μεταξύ τους, οδηγώντας έτσι στην αποκάλυψη της ταυτότητάς της.
- Μη-*παρατηρησιμότητα (Unobservability)*: η διαδικασία μέσω της οποία προστατεύεται η ιδιωτικότητα μιας οντότητας από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να παρατηρήσουν ή να εντοπίσουν ίχνη της πρώτης.

3.2 Νομικό-Κανονιστικό Πλαίσιο Προστασίας της Ιδιωτικότητας και Προσωπικών Δεδομένων

Μπορεί το δικαίωμα στην προστασία των προσωπικών δεδομένων να μην ταυτίζεται με το δικαίωμα στην ιδιωτική ζωή, ωστόσο η αξία της δικανικής αναγνώρισής του εντοπίζεται στην αξία της προστασίας της ιδιωτικότητας του ατόμου. Η αξία της ιδιωτικότητας έγκειται στην ικανότητα της να παρέχει στο πρόσωπο προστασία από κάθε εισβολή ή παρέμβαση στον ιδιωτικό του χώρο, καθώς και από κάθε είδους καταπιεστική, χειραγωγική, ελεγκτική ή πατερναλιστική συμπεριφορά, η οποία στοχεύει στον περιορισμό της ελευθερίας του προσώπου να αναπτύσσει απρόσκοπτα την προσωπικότητά του και της αυτονομίας του να διαμορφώνει και να απολαμβάνει τις σχέσεις του με τους οικείους του, καθώς και τις επιλογές εκείνες μέσα από τις οποίες τελικά αυτοπροσδιορίζεται (Ακριβοπούλου, 2009). Στο πλαίσιο αυτό, η προστασία του δικαιώματος στην ιδιωτική ζωή εξασφαλίζει σαν αόρατη ασπίδα στο πρόσωπο ότι η ταυτότητα, η αξιοπρέπεια του, η δυνατότητα του να υιοθετεί εναλλακτικές μορφές ζωής (όσον αφορά την σεξουαλικότητα ή τις σχέσεις οικειότητάς του) προστατεύονται από κάθε κριτική, χειραγωγική ή εξευτελιστική συμπεριφορά

3.2.1 Κατευθυντήριες Αρχές που διέπουν την Προστασία της Ιδιωτικότητας

Οι βασικές αρχές που πρέπει να διέπουν την προστασία των προσωπικών δεδομένων, όπως ορίστηκαν από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης, στις Κατευθυντήριες Οδηγίες για την Προστασία της Ιδιωτικότητας και τη Διασυνοριακή Ροή των Προσωπικών Δεδομένων (OECD, 1980) και που, περισσότερο ή λιγότερο, αντανακλώνται σε όλους τους σύγχρονους σχετικούς νόμους των δημοκρατικών κρατών παγκοσμίως, είναι οι παρακάτω:

- *Αρχή περιορισμού της συλλογής (Collection Limitation Principle):* Θα πρέπει να υπάρχουν όρια στη συλλογή προσωπικών δεδομένων, η συλλογή τους θα πρέπει να πραγματοποιείται με χρήση θεμιτών και σύννομων μέσων και – όπου είναι δυνατό – με τη συναίνεση ή την ενημέρωση του χρήστη.
- *Αρχή ποιότητας των δεδομένων (Data Quality Principle):* Τα προσωπικά δεδομένα θα πρέπει να είναι σχετικά με το σκοπό για τον οποίο πρόκειται να χρησιμοποιηθούν ενώ – στο βαθμό που είναι απαραίτητο για το σκοπό αυτό – θα πρέπει να είναι πλήρη, ακριβή και ενημερωμένα.
- *Αρχή προσδιορισμού του σκοπού (Purpose Specification Principle):* Ο σκοπός για τον οποίο συλλέγονται προσωπικά δεδομένα θα πρέπει να προσδιορίζεται το αργότερο κατά τη χρονική στιγμή της συλλογής τους, ενώ η συνακόλουθη χρήση τους θα πρέπει να περιορίζεται στην εκπλήρωση του σκοπού αυτού ή κάποιου πλήρως συμβατού σκοπού.
- *Αρχή περιορισμού της χρήσης (Use Limitation Principle)*: Τα προσωπικά δεδομένα δε θα πρέπει να κοινοποιούνται σε τρίτες οντότητες ή να χρησιμοποιούνται για άλλο σκοπό εκτός από τον προσδιορισμένο, σύμφωνα με την αρχή προσδιορισμού του σκοπού, εκτός εάν υπάρχει η σχετική συναίνεση του χρήστη ή η εξουσιοδότηση από το νόμο.
- *Αρχή προστασίας της ασφάλειας (Security Safeguards Principle)*: Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται με χρήση των κατάλληλων μηχανισμών απέναντι σε κινδύνους, όπως η μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, τροποποίηση ή κοινοποίηση σε τρίτες οντότητες.
- *Αρχή της διαφάνειας (Openness Principle):* Θα πρέπει να υπάρχει γενική διαφάνεια αναφορικά με τις πολιτικές και τις πρακτικές που σχετίζονται

με τη συλλογή και επεξεργασία των προσωπικών δεδομένων, καθώς και με την ταυτότητα του φορέα που διενεργεί τη συλλογή και επεξεργασία.

- *Αρχή της συμμετοχής του ατόμου (Individual Participation Principle):* Το κάθε άτομο θα πρέπει να έχει το δικαίωμα:
    - Να αποκτά είτε απ' ευθείας από τον υπεύθυνο της επεξεργασίας είτε μέσω κάποιου άλλου τρόπου, επιβεβαίωση αναφορικά με το αν ο υπεύθυνος της επεξεργασίας διαθέτει δεδομένα που σχετίζονται με το εν λόγω άτομο.
    - Να του ανακοινώνονται δεδομένα που σχετίζονται με αυτό, μέσα σε εύλογο χρονικό διάστημα, με εύλογο τρόπο, σε μορφή εύκολα κατανοητή και εφόσον η ανακοίνωση προϋποθέτει κόστος, αυτό να μην είναι υπερβολικό.
    - Να του παρέχονται οι λόγοι για τους οποίους απορρίπτονται αιτήσεις του που αναφέρονται στις δύο παραπάνω παραγράφους και να διατηρεί στην περίπτωση αυτή τη δυνατότητα της αμφισβήτησης, της απόρριψης και της περαιτέρω διεκδίκησης.
    - Να αμφισβητεί προσωπικά δεδομένα που σχετίζονται με αυτό, και, σε περίπτωση επιτυχημένης αμφισβήτησης, να μπορεί να προχωρεί σε εξάλειψη, διόρθωση ή ολοκλήρωση των δεδομένων αυτών.
- *Αρχή της ευθύνης (Accountability Principle):* Κάθε υπεύθυνος της επεξεργασίας δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι υπόλογος, αναφορικά με την εφαρμογή των μέτρων εκείνων που προάγουν τις παραπάνω αρχές, που πρέπει να διέπουν την προστασία των προσωπικών δεδομένων.

Στις παραπάνω βασικές αρχές για την προστασία των προσωπικών δεδομένων βασίστηκε, μεταξύ άλλων, και η ανάπτυξη της Ευρωπαϊκής Οδηγίας 95/46/ΕΚ , η οποία παρουσιάζεται στη συνέχεια.

3.2.2 Ευρωπαϊκή Οδηγία 1995/46/ΕΚ

Η Ευρωπαϊκή Οδηγία 95/46/ΕΚ έχει ως σκοπό την προστασία των ατομικών δικαιωμάτων και ελευθεριών, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, και την ελεύ-

θερη κυκλοφορία των δεδομένων αυτών. Προσδιορίζει έναν κατάλογο περιπτώσεων, στις οποίες επιτρέπεται η επεξεργασία προσωπικών δεδομένων, με βάση την αντίληψη ότι η επεξεργασία επιτρέπεται μόνο σε περιπτώσεις, όπου σταθμίζονται τα δικαιώματα και τα δημόσια ή ιδιωτικά συμφέροντα. Πιο συγκεκριμένα, η επεξεργασία επιτρέπεται μόνον εφόσον:

- Πραγματοποιείται έπειτα από σχετική συγκατάθεση (*Consent*) από το υποκείμενο των δεδομένων (*Data Subject*),
- Εντάσσεται στο πλαίσιο της εκπλήρωσης μιας συμβατικής σχέσης στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος,
- Είναι αναγκαία για την εκπλήρωση υποχρέωσης από το νόμο,
- Αποσκοπεί στη διαφύλαξη ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται τα δεδομένα,
- Είναι απαραίτητη για την ικανοποίηση του έννομου συμφέροντος του υπεύθυνου επεξεργασίας, εφόσον δεν προέχει το συμφέρον του υποκειμένου των δεδομένων.

Οι διατάξεις της Οδηγίας 95/46/ΕΚ για την επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα, ξεκινούν από την απαγόρευση της επεξεργασίας τους. Η απαγόρευση αίρεται αποκλειστικά στην περίπτωση ενός καταλόγου εξαιρέσεων που περιλαμβάνει τις περιπτώσεις:

- το υποκείμενο των δεδομένων να έχει δώσει ρητά τη συγκατάθεσή του για την επεξεργασία,
- η επεξεργασία να είναι απαραίτητη προκειμένου να εκπληρωθούν οι υποχρεώσεις και τα ειδικά δικαιώματα του υπευθύνου της επεξεργασίας στον τομέα του εργατικού δικαίου, στο βαθμό που το επιτρέπει η εθνική νομοθεσία, η οποία προβλέπει επαρκείς εγγυήσεις,
- η επεξεργασία να είναι απαραίτητη για τη διασφάλιση ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου προσώπου, αν ο ενδιαφερόμενος τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του,
- η επεξεργασία να πραγματοποιείται από ίδρυμα, σωματείο ή οποιονδήποτε άλλο μη κερδοσκοπικό φορέα, ο οποίος επιδιώκει πολιτικούς, φιλοσοφικούς, θρησκευτικούς ή συνδικαλιστικούς σκοπούς,
- η επεξεργασία να αφορά σε δεδομένα τα οποία προδήλως δημοσιοποιούνται από το πρόσωπο στο οποίο αναφέρονται, ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου,

- η επεξεργασία των δεδομένων να είναι αναγκαία για την ιατρική πρόληψη ή διάγνωση, την παροχή ιατροφαρμακευτικής αγωγής ή τη διαχείριση των ιατροφαρμακευτικών υπηρεσιών.

Τέλος, η επεξεργασία δεδομένων σχετικών με παραβάσεις, ποινικές καταδίκες ή μέτρα ασφαλείας επιτρέπεται μόνον υπό τον έλεγχο της εθνικής δημόσιας αρχής. Η βασική αντίληψη που διέπει την Οδηγία 95/46/ΕΚ είναι ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να περιορίζεται στο ελάχιστο δυνατό. Οι δύο κύριες αρχές που σχετίζονται με τον περιορισμό αυτό είναι η "αρχή του σκοπού" και η "αρχή της αναλογικότητας". Η αρχή του σκοπού επιτάσσει, ο σκοπός της επεξεργασίας να είναι σαφής, νόμιμος και γνωστός στο υποκείμενο των δεδομένων. Με αυτό τον τρόπο οριοθετεί τις δυνατότητες επέμβασης και συλλογής, περιορίζει την εμβέλεια της επεξεργασίας και προσδιορίζει τη διάρκειά της. Θα πρέπει να σημειωθεί ότι η συγκατάθεση του υποκειμένου των δεδομένων λαμβάνεται αποκλειστικά σε σχέση με ένα συγκεκριμένο σκοπό επεξεργασίας. Η δεύτερη αρχή αναφέρεται στην "αρχή της αναλογικότητας", που επιβάλλει τα δεδομένα να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς, οι οποίοι είναι γνωστοί στο υποκείμενο των δεδομένων, και η μεταγενέστερη επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς. Η Οδηγία 95/46/ΕΚ, λοιπόν, προσδιορίζει ένα σύνολο από ποιοτικές προδιαγραφές που πρέπει να πληρούνται κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Οι αρχές αυτές είναι:

- επιταγή για σύννομη και θεμιτή επεξεργασία,
- η τήρηση της "αρχής του σκοπού", δηλαδή η απαίτηση τα δεδομένα να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς, οι οποίοι είναι γνωστοί στο υποκείμενο των δεδομένων, και η επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς,
- η τήρηση της "αρχής της αναλογικότητας", δηλαδή τα δεδομένα να είναι κατάλληλα, συναφή προς το θέμα και όχι υπερβολικά, σε σχέση με τους σκοπούς για τους οποίους συλλέγονται και υφίστανται επεξεργασία,
- η απαίτηση τα δεδομένα να είναι ακριβή. Εφόσον χρειάζεται ενημέρωση, πρέπει να λαμβάνονται όλα τα εύλογα μέτρα, ώστε δεδομένα τα οποία είναι ανακριβή ή ελλιπή, έπειτα από την επεξεργασία, σε σχέση με τους σκοπούς για τους οποίους έχουν συλλεχθεί ή τηρούνται, να διαγράφονται ή να διορθώνονται,

- η απαίτηση να διατηρούνται με μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των προσώπων στα οποία αναφέρονται, μόνο κατά τη διάρκεια περιόδου που δεν υπερβαίνει την απαιτούμενη για την επίτευξη των σκοπών για τους οποίους έχουν συλλεχθεί ή για τους οποίους αργότερα υφίστανται επεξεργασία.

Ο υπεύθυνος της επεξεργασίας πρέπει να παρέχει στο πρόσωπο από το οποίο συλλέγονται δεδομένα που το αφορούν τουλάχιστον τις εξής πληροφορίες: την ταυτότητα του υπευθύνου της επεξεργασίας, τους σκοπούς της επεξεργασίας, για την οποία προορίζονται τα δεδομένα, και οποιαδήποτε περαιτέρω πληροφορία, όπως τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων, το κατά πόσον η παροχή των δεδομένων είναι υποχρεωτική ή όχι, καθώς και τις ενδεχόμενες συνέπειες της άρνησης παροχής τους, την ύπαρξη δικαιώματος πρόσβασης στα συγκεκριμένα δεδομένα και δικαιώματος διόρθωσής τους.

Στην περίπτωση που τα δεδομένα δεν έχουν συλλεχθεί από το πρόσωπο το οποίο αφορούν, η Οδηγία προβλέπει ότι, όταν αυτά καταχωρηθούν ή εάν προβλέπεται ανακοίνωσή τους σε τρίτους (το αργότερο κατά την πρώτη ανακοίνωσή τους), το υποκείμενο των δεδομένων θα πρέπει να ενημερωθεί από τον υπεύθυνο επεξεργασίας για τις παραπάνω πληροφορίες. Πέρα από την υποχρέωση ενημέρωσης, η Οδηγία απαιτεί από τα Κράτη-Μέλη να διαφυλάσσουν το δικαίωμα πρόσβασης του υποκειμένου των δεδομένων ελεύθερα και απεριόριστα, σε εύλογα διαστήματα και χωρίς υπερβολική καθυστέρηση ή δαπάνη. Συγκεκριμένα, το υποκείμενο των δεδομένων θα πρέπει να μπορεί να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για την ύπαρξη ή μη επεξεργασίας, το σκοπό της, τις κατηγορίες των δεδομένων του που υποβάλλονται σε επεξεργασία και τους αποδέκτες των δεδομένων. Επίσης, θα πρέπει να λαμβάνει επιβεβαίωση για τη γνωστοποίηση των δεδομένων υπό επεξεργασία καθώς και των διαθέσιμων πληροφοριών σχετικά με την προέλευσή τους και τη λογική στην οποία στηρίζεται κάθε αυτοματοποιημένη επεξεργασία των δεδομένων. Τέλος, το υποκείμενο των δεδομένων έχει το δικαίωμα να αντιτάσσεται στην επεξεργασία των προσωπικών του δεδομένων για επιτακτικούς και νόμιμους λόγους, σύμφωνα με τις ειδικές διατάξεις του Άρθρου 14 της Οδηγίας 95/46/ΕΚ.

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα που έχουν υποστεί επεξεργασία ή πρόκειται να υποστούν επεξεργασία μετά τη διαβίβασή τους από τα Κράτη-Μέλη προς τρίτες χώρες, επιτρέπεται μόνον αν η εν λόγω τρίτη χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Το επίπεδο προστασίας που παρέχει η τρίτη χώρα σχετίζεται με τη φύση των δεδομένων, το σκοπό και τη διάρκεια της επεξεργασίας, τη χώρα προέλευσης και τελικού προορισμού, τις εθνι-

κές διατάξεις και τα μέτρα ασφάλειας για την προστασία προσωπικών δεδομένων στην τρίτη χώρα. Στην περίπτωση που διαπιστωθεί από τα Κράτη-Μέλη και την Ευρωπαϊκή Επιτροπή ότι μία τρίτη χώρα δεν παρέχει ικανοποιητικό επίπεδο προστασίας ενημερώνονται αμοιβαία και τα Κράτη-Μέλη λαμβάνουν τα αναγκαία μέτρα ώστε να αποφευχθεί οποιαδήποτε διαβίβαση τέτοιου είδους δεδομένων προς την εν λόγω τρίτη χώρα.

3.2.3 Ευρωπαϊκή Οδηγία 2002/58/ΕΚ

Η Ευρωπαϊκή Οδηγία 2002/58/ΕΚ έχει σκοπό την διασφάλιση ισοδύναμου επιπέδου προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως το δικαίωμα στην ιδιωτική ζωή, σε σχέση με την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών. Επίσης, αποσκοπεί στη διασφάλιση της ελεύθερης κυκλοφορίας των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στα Κράτη-Μέλη της Κοινότητας. Εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στα πλαίσια της παροχής διαθέσιμων στο κοινό υπηρεσιών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικής επικοινωνίας στα Κράτη-Μέλη της Ε. Έ.

Οι βασικές έννοιες των ρυθμίσεων της Οδηγίας είναι:

- *Χρήστης*: κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της υπηρεσίας
- *Δεδομένα κίνησης*: τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της
- *Δεδομένα Θέσης*: τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών
- *Επικοινωνία*: κάθε πληροφορία που ανταλλάσσεται ή διαβιβάζεται μεταξύ ενός πεπερασμένου αριθμού μερών, μέσω μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών

Η Οδηγία προβλέπει για τα Κράτη-Μέλη να κατοχυρώνουν μέσω εθνικής νομοθεσίας το απόρρητο των επικοινωνιών που διενεργούνται μέσω του δημοσίου δικτύου επικοινω-

νιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης. Στο πλαίσιο του απορρήτου των επικοινωνιών, απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεση των ενδιαφερομένων τελευταίων. Παρόλα αυτά διευκρινίζεται ότι δεν απαγορεύεται η τεχνική αποθήκευση, η οποία είναι αναγκαία για τη διαβίβαση επικοινωνίας, με την επιφύλαξη της αρχής του απορρήτου. Τα δεδομένα κίνησης είναι τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της. Τα δεδομένα κίνησης μπορεί, μεταξύ άλλων, να αναφέρονται στη δρομολόγηση, στη διάρκεια, στο χρόνο ή στο μέγεθος μιας επικοινωνίας, στο πρωτόκολλο που χρησιμοποιείται, στη θέση του τερματικού εξοπλισμού του πομπού ή του δέκτη, στο δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία, στην αρχή, το τέλος ή τη διάρκεια μιας σύνδεσης. Η Οδηγία επιτρέπει την επεξεργασία δεδομένων κίνησης, εφόσον είναι απαραίτητα για τη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων, αλλά μόνο ως το τέλος της χρονικής περιόδου εντός της οποίας δύναται να αμφισβητείται νομίμως ο λογαριασμός ή να επιδιώκεται η πληρωμή. Η επεξεργασία και τεχνική αποθήκευση των δεδομένων κίνησης μετά την ολοκλήρωση του σκοπού της επεξεργασίας (π.χ. σύνδεση) επιτρέπεται έπειτα από την "ανωνυμοποίησή" (*Anonymization*) τους.

Τα δεδομένα θέσης αναφέρονται στα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Τα δεδομένα θέσης μπορεί να αναφέρονται στο γεωγραφικό πλάτος, το γεωγραφικό μήκος και το υψόμετρο του τερματικού εξοπλισμού του χρήστη, στην κατεύθυνση της κίνησής του, στον προσδιορισμό της γεωγραφικής ζώνης του δικτύου στο οποίο βρίσκεται ο τερματικός εξοπλισμός σε μια δεδομένη χρονική στιγμή κ.α. Η επεξεργασία των δεδομένων θέσης επιτρέπεται μόνον όταν αυτά καθίστανται ανώνυμα, ή με τη ρητή συγκατάθεση των χρηστών ή συνδρομητών στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια για την παροχή μιας υπηρεσίας προστιθέμενης αξίας. Για να δώσει τη συγκατάθεσή του ο χρήστης ή συνδρομητής είναι υποχρεωμένος ο φορέας παροχής υπηρεσιών να τον ενημερώσει σχετικά με τον τύπο των δεδομένων θέσης, τους σκοπούς και τη διάρκεια της εν λόγω επεξεργασίας, καθώς και το ενδεχόμενο μετάδοσής τους σε τρίτους για το σκοπό παροχής της υπηρεσίας προστιθέμενης αξίας. Ο χρήστης μπορεί να ανακαλέσει οποτεδήποτε τη συγκατάθεσή του.

Ένα από τα σημαντικά ζητήματα που διευθετεί η Οδηγία είναι η χρήση λογισμικού παρακολούθησης - ακρόασης και κρυφών αναγνωριστικών στοιχείων που μπορεί να εγκατασταθούν στο τερματικό του χρήστη, χωρίς αυτός να το γνωρίζει, με σκοπό την πρόσβαση σε πληροφορίες, την αποθήκευση αθέατων πληροφοριών ή την ανίχνευση των δραστηριοτήτων του. Η παρακολούθηση αυτή συνιστά ενδεχόμενη παραβίαση της ιδιωτικής ζωής του χρήστη. Η χρησιμοποίηση των πληροφοριών είναι νόμιμη μόνο για θεμιτούς σκοπούς (π.χ. η ανάλυση αποτελεσματικότητας του σχεδιασμού και της παρουσίασης μιας ιστοσελίδας) και εφόσον προηγουμένως έχει προηγηθεί η αντίστοιχη ενημέρωση.

3.2.4 Ευρωπαϊκή Οδηγία 2006/24/ΕΚ

Η Οδηγία 2006/24/ΕΚ, επιπλέον των Οδηγιών 95/46/ΕΚ και 2002/58/ΕΚ, παρέχει οδηγίες στα Κράτη-Μέλη αναφορικά με τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία, σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών. Αποβλέπει στην εναρμόνιση των διατάξεων των Κρατών-Μελών σχετικά με τις υποχρεώσεις των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό ή δημοσίου δικτύου επικοινωνιών, όσον αφορά στη διατήρηση ορισμένων δεδομένων που παράγονται ή υφίστανται επεξεργασία από αυτούς, ώστε να διασφαλιστεί ότι τα δεδομένα καθίστανται διαθέσιμα για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων. Η Οδηγία αφορά σε δεδομένα κίνησης και θέσης, στις νομικές οντότητες και στα φυσικά πρόσωπα και στα συναφή δεδομένα που απαιτούνται για την αναγνώριση του συνδρομητή ή του καταχωρημένου χρήστη. Δεν εφαρμόζεται στο περιεχόμενο των ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των πληροφοριών στις οποίες η πρόσβαση πραγματοποιείται με τη χρήση δικτύου ηλεκτρονικών επικοινωνιών. Κατά παρέκκλιση συγκεκριμένων ρυθμίσεων της Οδηγίας 2002/58/ΕΚ, η Οδηγία 2006/24/ΕΚ ορίζει ότι τα Κράτη-Μέλη πρέπει να θεσπίζουν μέτρα, ώστε να διασφαλίζεται ότι τα δεδομένα διατηρούνται, εφόσον παράγονται ή υποβάλλονται σε επεξεργασία από παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, στο πλαίσιο της δικαιοδοσίας τους κατά την παροχή των συγκεκριμένων υπηρεσιών επικοινωνιών.

Η Οδηγία προσδιορίζει έναν κατάλογο κατηγοριών και τύπων δεδομένων που πρέπει να διατηρούνται από τους παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών. Οι κατηγορίες δεδομένων είναι:

- Δεδομένα αναγκαία για την ανίχνευση και τον προσδιορισμό της πηγής της επικοινωνίας,
- Δεδομένα αναγκαία για τον προσδιορισμό του προορισμού της επικοινωνίας,
- Δεδομένα αναγκαία για τον προσδιορισμό της ημερομηνίας, ώρας και διάρκειας της επικοινωνίας,
- Δεδομένα αναγκαία για τον προσδιορισμό του είδους της επικοινωνίας
- Δεδομένα αναγκαία για τον προσδιορισμό του εξοπλισμού επικοινωνίας των χρηστών, ή του φερομένου ως εξοπλισμού επικοινωνίας τους, για παράδειγμα οι τηλεφωνικοί αριθμοί καλούντος και καλουμένου,
- Δεδομένα αναγκαία για τον προσδιορισμό της θέσης του εξοπλισμού κινητής επικοινωνίας.

Επακριβώς τα δεδομένα που πρέπει να τηρούνται σε κάθε κατηγορία απαριθμούνται και προσδιορίζονται εξαντλητικά στην Οδηγία. Τα Κράτη-Μέλη πρέπει να διασφαλίζουν ότι οι κατηγορίες δεδομένων που προσδιορίστηκαν διατηρούνται για χρονικό διάστημα όχι μικρότερο του εξαμήνου και όχι μεγαλύτερο της διετίας από την ημερομηνία της επικοινωνίας.

3.2.5 Ελληνικό Κανονιστικό Πλαίσιο

Η Ελλάδα υπήρξε από τις πρώτες χώρες που μετέφεραν την κοινοτική Οδηγία 95/46/ΕΚ στο εσωτερικό δίκαιο. Ήδη από το 1985 είχαν εκπονηθεί σχετικά προσχέδια νόμου και μάλιστα είχαν κατατεθεί στο Κοινοβούλιο σχέδια και προτάσεις νόμου, τα οποία όμως δεν τελεσφόρησαν (Μήτρου, 2010). Το ελληνικό νομοθετικό πλαίσιο για την προστασία προσωπικών δεδομένων συγκροτείται από το συνταγματικό δικαίωμα προστασίας προσωπικών δεδομένων όπως κατοχυρώνεται στο άρθρο 9 Α του Συντάγματος, τον νόμο 2472/97 (ΦΕΚ Α' 50/10.04.1997) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως ισχύει μετά τις τροποποιήσεις που κατά καιρούς εισήχθησαν, καθώς και τον νόμο 3471/06 (ΦΕΚ Α' 133/28.06.2006) που – εκτός των τροποποιήσεων που επέφερε στον Ν. 2472/97 – αφορά στην προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Μήτρου, 2010).

3.2.6 Νομικό Πλαίσιο για την Προστασία του Ατόμου Από την Επεξεργασία Προσωπικών Δεδομένων

Ο Ν. 2472/97 μετέφερε τις ρυθμίσεις της Οδηγίας 95/46/ΕΚ για την προστασία δεδομένων στην ελληνική έννομη τάξη. Αντικείμενό του είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Σκοπός του είναι η προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Ο νομοθέτης οριοθετεί με ουσιαστικούς, οργανωτικούς, διαδικαστικούς και κυρωτικούς κανόνες τη συνταγματικά ανεκτή επεξεργασία προσωπικών δεδομένων και με τον τρόπο αυτό ρυθμίζει τη ροή των προσωπικών δεδομένων στο πλαίσιο του κράτους, της οικονομίας και της κοινωνίας και οργανώνει τις πληροφοριακές σχέσεις μεταξύ των προσώπων (Μήτρου, 2010).

Ως επεξεργασία προσωπικών δεδομένων ορίζεται κάθε εργασία ή σειρά εργασιών που πραγματοποιείται από το δημόσιο ή από νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου ή από ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα. Ο υπεύθυνος επεξεργασίας είναι οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.

Ο Ν. 2472/97 ενσωματώνει τις ρυθμίσεις της Οδηγίας 95/46/ΕΚ επιτρέποντας την επεξεργασία δεδομένων προσωπικού χαρακτήρα στις περιπτώσεις όπου:

- Το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του,
- Εντάσσεται στο πλαίσιο της εκπλήρωσης μίας συμβατικής σχέσης στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος Είναι αναγκαία για την εκπλήρωση υποχρέωσης από το νόμο,
- Αποσκοπεί στη διαφύλαξη ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται τα δεδομένα,
- Είναι απαραίτητη για την εκπλήρωση έργου δημοσίου συμφέροντος και
- Κρίνεται αναγκαία για την ικανοποίηση του έννομου συμφέροντος του υπεύθυνου επεξεργασίας, εφόσον δεν προέχει το συμφέρον του υποκειμένου των δεδομένων.

Στην περίπτωση επεξεργασίας προσωπικών δεδομένων σύμφωνα με τις διατάξεις του Ν. 2472/97, ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή Προστασίας Προσωπικών δεδομένων τη σύσταση και λειτουργία αρχείου ή την έναρξη της επε-

ξεργασίας. Επίσης, απαγορεύει την επεξεργασία ευαίσθητων προσωπικών δεδομένων. Η απαγόρευση αυτή αίρεται αποκλειστικά στην περίπτωση ενός καταλόγου εξαιρέσεων που περιλαμβάνει τις περιπτώσεις:

- το υποκείμενο των δεδομένων να έχει δώσει γραπτή συγκατάθεση για την επεξεργασία,
- η επεξεργασία να πραγματοποιείται για ερευνητικούς και επιστημονικούς αποκλειστικά σκοπούς και υπό τον όρο ότι τηρείται η ανωνυμία και λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων,
- η επεξεργασία να είναι απαραίτητη για τη διασφάλιση ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου προσώπου, αν ο ενδιαφερόμενος τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του,
- η επεξεργασία να αφορά δεδομένα τα οποία προδήλως δημοσιοποιούνται από το πρόσωπο στο οποίο αναφέρονται, ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου,
- η επεξεργασία των δεδομένων να είναι αναγκαία για την ιατρική πρόληψη ή διάγνωση, την παροχή ιατροφαρμακευτικής αγωγής ή τη διαχείριση των ιατροφαρμακευτικών υπηρεσιών,
- η επεξεργασία να αφορά δεδομένα δημοσίων προσώπων, εφόσον αυτά συνδέονται με την άσκηση δημοσίου λειτουργήματος ή τη διαχείριση συμφερόντων τρίτων και να πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος.

Ο Ν. 2472/97 ορίζει ότι η επεξεργασία των δεδομένων πρέπει να ακολουθεί τις αρχές ποιότητας των δεδομένων όπως προσδιορίζονται στην Οδηγία 95/46/ΕΚ και υιοθετεί την αρχή διαφάνειας της επεξεργασίας, ορίζοντας το δικαίωμα του υποκειμένου για ενημέρωση της επεξεργασίας των δεδομένων, δικαίωμα πρόσβασης στις πληροφορίες που αφορούν την επεξεργασία και δικαίωμα αντίρρησης στην επεξεργασία.

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα επιτρέπεται ελεύθερα ανάμεσα στα Κράτη-Μέλη της Ε.Ε. Στην περίπτωση διαβίβασης δεδομένων προς κράτη που δεν είναι μέλη της Ευρωπαϊκής Ένωσης είναι απαραίτητη σχετική άδεια από την Αρχή Προστασίας Προσωπικών Δεδομένων η οποία χορηγεί άδεια λαμβάνοντας υπόψη:

- τη φύση των δεδομένων,

- τους σκοπούς και τη διάρκεια της επεξεργασίας,
- την αντίστοιχη νομοθεσία και κώδικες δεοντολογίας,
- τα μέτρα ασφαλείας για την προστασία δεδομένων προσωπικού χαρακτήρα και
- το επίπεδο προστασίας των χωρών προέλευσης, διέλευσης και τελικού προορισμού των δεδομένων

Αντίστοιχα, η διασύνδεση αρχείων που περιέχουν δεδομένα προσωπικού χαρακτήρα και τα οποία εξυπηρετούν διαφορετικούς σκοπούς, επιτρέπεται, έπειτα από κοινή δήλωση των υπευθύνων επεξεργασίας στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Στην περίπτωση που κάποιο από τα αρχεία περιέχει ευαίσθητα δεδομένα απαιτείται ειδική άδεια από την Αρχή.

3.3 Τα Όρια και οι Προκλήσεις της Προάσπισης της Ιδιωτικότητας

Η προστασία των προσωπικών δεδομένων δεν μπορεί παρά να αποτελεί εγγενές στοιχείο της νέας πληροφοριακής έννομης τάξης, καθώς διαμορφώνεται σταδιακά και σύστοιχα προς την εξελισσόμενη Εποχή της Πληροφορίας (*Information Age*). Τα όρια της ιδιωτικότητας και της προστασίας της καθορίζονται από τεχνολογικούς παράγοντες, την παγκοσμιοποίηση της επεξεργασίας και της επικοινωνίας, τις αλλαγές των αντιλήψεων τόσο των ατόμων όσο και των κρατικών και κοινωνικών δομών ως προς το περιεχόμενο της ιδιωτικότητας όσο και ως προς τη σχέση της με άλλα δημόσια και ιδιωτικά αγαθά και επιδιώξεις. Η πληροφοριακή ιδιωτικότητα διάγει περίοδο κρίσεως που οφείλεται τόσο στην υφιστάμενη κατάσταση όσο και σε βασικά δομικά χαρακτηριστικά των ΤΠΕ, όπως αυτές εξελίσσονται και λειτουργούν. Οι νέες τεχνολογίες είναι προϊόν της κοινωνίας, η προέλευση και η εξέλιξή τους προσδιορίζονται από αυτή, όμως από την άλλη πλευρά επηρεάζουν, ενίοτε δε, καθορίζουν την εξέλιξη της κοινωνίας και των θεσμών της. Η ανάπτυξη των τεχνολογιών της πληροφορίας και επικοινωνίας με την αλματώδη πρόοδό τους αλλάζουν το τοπίο: στη νέα κοινωνία της πληροφορίας οι υπηρεσίες που προσφέρονται από τις νέες τεχνολογίες, συνιστούν κρίσιμο παράγοντα καθορισμού των κοινωνικών και οικονομικών δομών και σχέσεων (Μήτρου, 2010).

3.3.1 Ιδιωτικότητα, Απόρρητο και Ασφάλεια

Μία από τις συνηθέστερες θεωρήσεις της έννοιας της ιδιωτικότητας είναι ότι συνίσταται στον απόρρητο χαρακτήρα ορισμένων ζητημάτων και υπό αυτήν την έννοια η ιδιωτικότητα

προσβάλλεται με την αποκάλυψη απόρρητης πληροφορίας. Ιδίως η «κλασική» προσέγγιση της ιδιωτικότητας ως καταφυγίου (*Refugium*) παρουσιάζει στοιχεία ταύτισης ή και σύγχυσης με την έννοια του απορρήτου (*Secrecy*) και της εμπιστευτικότητας (*Confidentiality*). Οι όροι αυτοί, αν και συχνά γίνονται αντιληπτοί και χρησιμοποιούνται ως ισοδύναμοι, εκφράζοντας σε τελευταία ανάλυση παρεμφερείς αξιώσεις προστασίας, εντούτοις δεν ταυτίζονται: Η έννοια του απορρήτου (*Secrecy*) αναφέρεται είτε στη μη προσπελασιμότητα ορισμένων πληροφοριών που εμπίπτουν στη σφαίρα επιρροής ενός ατόμου είτε στο καθήκον ή την υποχρέωση προσώπων ή οργανισμών να διαφυλάσσουν πληροφορίες, που είτε ένα άτομο έχει εμπιστευτεί σε αυτά, στο πλαίσιο μιας γενικότερης σχέσης εμπιστοσύνης (όπως το *ιατρικό απόρρητο* ή το *τραπεζικό απόρρητο*), είτε τις κατέχουν επί τη βάσει της θέσης και της αρμοδιότητάς τους (όπως το *υπηρεσιακό απόρρητο*). Εάν μάλιστα πρόκειται για πληροφορία που εμπίπτει στη δημόσια σφαίρα δεν είναι νοητή η προστασία από το απόρρητο. Για να είναι απόρρητη/εμπιστευτική η πληροφορία θα πρέπει να είναι σε μία κατάσταση περιορισμένης προσβασιμότητας από πρόσωπα, ομάδες κ.λπ. (Μήτρου, 2010). Προς αυτή την κατεύθυνση επιχειρείται για πρώτη φορά μία ολοκληρωμένη επισκόπηση και καταγραφή των βασικών παραμέτρων για την αποτίμηση της επικινδυνότητας (*Risk Assessment*), δια της ανάλυσης τόσο των δυνητικών απειλών (*Threats*) που υφίστανται οι συναλλαγές των πολιτών και των επιχειρήσεων σε περιβάλλον υπηρεσιών ηλεκτρονικής διακυβέρνησης, όσο και των αρνητικών επιπτώσεων (*Impact*) που μπορούν να προκληθούν στον πάροχο της υπηρεσίας ή και στο χρήστη.

3.4 Ανάλυση Απειλών – Επιπτώσεων σε Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης

Ως απειλή μπορεί να θεωρηθεί οποιαδήποτε «*πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσοτέρων ιδιοτήτων-χαρακτηριστικών ασφάλειας ενός πληροφοριακού συστήματος*» (Λαμπρινουδάκης et al., 2010). Οι απειλές που εντοπίζονται στα πληροφοριακά συστήματα, δεν προέρχονται μόνον από κακόβουλες ενέργειες που προκαλούνται από εξωτερικές ή εσωτερικές οντότητες, αλλά συμπεριλαμβάνουν και σχεδιαστικά λάθη ή μη ηθελημένες ενέργειες που μπορούν να οδηγήσουν το πληροφοριακό σύστημα σε μη εκπλήρωση των στόχων του.

Η ανάλυση επικινδυνότητας (*Risk Analysis*) είναι η διαδικασία αναγνώρισης κινδύνων και ο υπολογισμός επικινδυνότητας. Η εκτίμηση επικινδυνότητας (*Risk Assessment*) είναι η διαδικασία αξιολόγησης της υπολογισμένης επικινδυνότητας σε σχέση με κριτήρια αξιολόγησης της

σημαντικότητάς της (Tsohou et al., 2010). Η συνολική διαδικασία ανάλυσης και εκτίμησης επικινδυνότητας αποτελεί την αποτίμηση επικινδυνότητας. Η αποτίμηση και διαχείριση επικινδυνότητας (*Risk Assessment and Management*) στηρίζεται στην αρχή ότι απόλυτη ασφάλεια δεν είναι δυνατό να υπάρξει, άρα το καλύτερο που μπορεί να γίνει είναι να εξισορροπηθεί η έκταση των πιθανών κινδύνων με το κόστος εφαρμογής των κατάλληλων αντιμέτρων (*Countermeasures*). Επομένως, χρειαζόμαστε μεθοδολογίες που να επιτρέπουν τη μέτρηση των κινδύνων και την έκφρασή τους σε κοινές μονάδες μέτρησης με την αποτελεσματικότητα των αντιμέτρων, ώστε να είναι δυνατή η σύγκρισή τους. Γι' αυτό το λόγο πρέπει να υπολογιστεί η επικινδυνότητα ενός συστήματος ως συνάρτηση των εξής παραγόντων:

- της αξίας των περιουσιακών του στοιχείων *(A)*
- της φύσης και του βαθμού των ευπαθειών του *(V)*
- της φύσης και της πιθανότητας εμφάνισης απειλών εναντίον του *(T)*
- της φύσης και έντασης των επιπτώσεων που θα έχουν οι απειλές αν πραγματοποιηθούν *(I)*

$$Επικινδυνότητα\ (Risk) = f(A, V, T, I)$$

3.4.1 Κατηγορίες Απειλών

Για την ολοκλήρωση μιας τυπικής συναλλαγής με μία Δημόσια Υπηρεσία, συνήθως απαιτείται η φυσική παρουσία του πολίτη ενώπιον ενός σχετικά εξουσιοδοτημένου δημόσιου υπαλλήλου. Στην περίπτωση αυτή, η διαδικασία της ταυτοποίησης πραγματοποιείται με τη φυσική παρουσία του πολίτη, ενώ η διαδικασία της αυθεντικοποίησης πραγματοποιείται με την προσκόμιση του κατάλληλου εγγράφου, το οποίο διαφοροποιείται ανάλογα με το είδος της συναλλαγής και τη Δημόσια Υπηρεσία. Για παράδειγμα, για την έκδοση Αποδεικτικού Φορολογικής Ενημερότητας (Α.Φ.Ε.) ή για την υποβολή Δήλωσης Φορολογίας Εισοδήματος απαιτείται η φυσική παρουσία του ενδιαφερομένου σε μία Δημόσια Οικονομική Υπηρεσία (Δ.Ο.Υ.), προκειμένου αυτός να ταυτοποιηθεί, και ακολουθεί επίδειξη εγγράφου από το οποίο προκύπτει ο Αριθμός Δελτίου Ταυτότητας (Α.Δ.Τ.) ή ο Αριθμός Διαβατηρίου (Α.Δ.) προκειμένου να αυθεντικοποιηθεί. Συνεπώς, αρχικά ο πολίτης ταυτοποιείται και στη συνέχεια αυθεντικοποιείται με την αξιοποίηση του κατάλληλου εγγράφου. Υπό το πρίσμα αυτό είναι σχεδόν ανέφικτο μία οντότητα να υποδυθεί μία άλλη. Ο τρόπος παράκαμψης αυτών των περιορισμών θα συμπεριλάμβανε είτε τη χρήση πλαστών

στοιχείων από τον ενδιαφερόμενο είτε την απουσία ουσιαστικού ελέγχου από την πλευρά του δημοσίου υπαλλήλου.

Αντιθέτως, στις υπηρεσίες ηλεκτρονικής διακυβέρνησης ένας δυνητικά κακόβουλος χρήστης δεν θα προσπαθήσει μόνο να εκμεταλλευτεί γνωστές ευπάθειες (*Vulnerabilities*) του συστήματος, αντίστοιχες με αυτές που εμφανίζονται στις υπηρεσίες Διαδικτύου, αλλά και στις συγκεκριμένες διαδικασίες εγγραφής, ταυτοποίησης και αυθεντικοποίησης, ανεξαρτήτως του τρόπου πραγματοποίησής τους, ηλεκτρονικά ή μη (Ramaraj & Mukerji, 2012). Συγκεκριμένα, ο επιτιθέμενος θα προσπαθήσει να επιτύχει έναν από τους ακόλουθους στόχους:

- Μη εξουσιοδοτημένη πρόσβαση
    - σε πληροφορία ή
    - στην παρεχόμενη υπηρεσία
- Αντιποίηση αρχής
    - εξουσιοδοτημένου χρήστη
    - υπηρεσίας
- Παραβίαση της ιδιωτικότητας και μη εξουσιοδοτημένη πρόσβαση ή χρήση των δεδομένων προσωπικού χαρακτήρα
- Άρνηση παροχής υπηρεσίας

Για παράδειγμα, στην περίπτωση όπου ένας πολίτης επιθυμεί να υποβάλλει Δήλωση Φορολογίας Εισοδήματος μέσω του Διαδικτύου, θα πρέπει να διασφαλιστούν συνθήκες αντίστοιχες με αυτές που ακολουθούνται στη συνήθη διαδικασία υποβολής σε κάποια Δ.Ο.Υ., με στόχο την ελαχιστοποίηση της πιθανότητας οι εμπλεκόμενες οντότητες να δράσουν κακόβουλα, εκμεταλλευόμενες κάποια σημεία ευπάθειας. Ακολούθως αναλύονται λεπτομερώς οι απειλές αυτές που είναι πιθανό να εκδηλωθούν σε επιθέσεις, ώστε να επιτευχθεί από τον κακόβουλο χρήστη κάποιος από τους προαναφερόμενους στόχους.

3.4.2 Απειλές Διακριτικών Αυθεντικοποίησης

Αρκετοί κίνδυνοι στα Π.Σ. που διαχειρίζονται ευαίσθητες πληροφορίες, προέρχονται από τη μη ορθή διαχείριση των διακριτικών αυθεντικοποίησης τόσο από τους χρήστες όσο και από την υπηρεσία που τα παρέχει. Σε αυτές τις περιπτώσεις, ο επιτιθέμενος προσπαθεί να αυθεντικοποιηθεί ως νόμιμος χρήστης και να έχει πρόσβαση σε πόρους του εξουσιοδοτημένου χρήστη (αντιποίηση αρχής), αξιοποιώντας κάποιο διακριτικό αυθεντικοποίησης του νόμιμου χρήστη, χω-

ρίς αυτό να έχει γίνει αντιληπτό από τον ίδιο. Οι απειλές για τα διακριτικά αυθεντικοποίησης κατηγοριοποιούνται με βάση τον τύπο του διακριτικού στα ακόλουθα:

- Κάτι που γνωρίζει ο νόμιμος χρήστης μπορεί να υποκλαπεί από τον επιτιθέμενο. Για παράδειγμα, ο επιτιθέμενος είναι δυνατό να ανακαλύψει το συνθηματικό ενός χρήστη πραγματοποιώντας επίθεση εξαντλητικής αναζήτησης (*Brute-Force Attack*). Οι πιο συνηθισμένοι τρόποι επίθεσης (Ferguson & Schneier, 2003) (Books LLC , 2010) στα συστήματα αυθεντικοποίησης με συνθηματικά είναι οι ακόλουθοι:
    - Επιθέσεις Αξιοποίησης Λεξικών,
    - Επιθέσεις Εξαντλητικής Αναζήτησης,
    - Επιθέσεις Τυχαίων Δοκιμών,
    - Υποκλοπή κατά τη μετάδοση των διαπιστευτηρίων και
    - Κοινωνική Μηχανική (*Social Engineering*)
- Κάτι που κατέχει ο νόμιμος χρήστης μπορεί να κλαπεί από τον επιτιθέμενο, να αντιγραφεί ή και να χρησιμοποιηθεί σε κάποια δοσοληψία, χωρίς ο νόμιμος χρήστης να το γνωρίζει. Για παράδειγμα, ο επιτιθέμενος μπορεί με τη χρήση κατάλληλου λογισμικού να υποκλέψει από το σύστημα του νόμιμου χρήστη το κρίσιμο διακριτικό που είναι αποθηκευμένο στο σκληρό δίσκο του χρήστη (π.χ. το ιδιωτικό του κλειδί).

3.4.3 Απειλές στα Πρωτόκολλα Αυθεντικοποίησης και στις Παρεχόμενες Υπηρεσίες

Οι πιο γνωστές απειλές που είναι δυνατό να εμφανιστούν στα πρωτόκολλα αυθεντικοποίησης και στις παρεχόμενες ηλεκτρονικά υπηρεσίες (Γκρίτζαλης et al., 2003) (Schneier et al., 2006) (Καμπουράκης et al., 2006) παρουσιάζονται παρακάτω και διαχωρίζονται ως ενεργές (*Active*) ή παθητικές (*Passive*), με βάση την ενεργή ή παθητική συμμετοχή του επιτιθέμενου:

- *Υποκλοπή επικοινωνίας-δεδομένων (Eavesdropping)*: Ο επιτιθέμενος σε αυτή την περίπτωση παρακολουθεί (*Eavesdrop*) το δίκτυο, για να καταγράψει τα μεταδιδόμενα δεδομένα, με δύο βασικούς στόχους:
    - την υποκλοπή δεδομένων (*Interception*): Για παράδειγμα ο επιτιθέμενος μπορεί να υποκλέψει δεδομένα συνομιλίας, μηνύματα ηλεκτρονικού ταχυδρομείου, κωδικούς κτλ.

- την ανάλυση των δεδομένων (*Traffic analysis*) και την αξιοποίησή τους σε μελλοντική επίθεση: Στην περίπτωση όπου τα δεδομένα που έχουν καταγραφεί είναι κρυπτογραφημένα, ο επιτιθέμενος είναι δυνατό να προσπαθήσει να αποκαλύψει το κλειδί κρυπτογράφησης, αξιοποιώντας για παράδειγμα εξαντλητική αναζήτηση κλειδιού. Η ανάλυση των δεδομένων, σε κάθε περίπτωση, έχει διαφορετικό στόχο ανάλογα με το σκοπό του επιτιθέμενου, όπως αποκάλυψη μυστικού κλειδιού ή εμπιστευτικών πληροφοριών.

- *Επιθέσεις ενδιάμεσου (Man-in-the-middle Attacks)*: Ο επιτιθέμενος σε αυτή την περίπτωση ενεργεί ως ενδιάμεσος, τροποποιώντας κατάλληλα τα αποστελλόμενα μηνύματα, προωθώντας τα στη συνέχεια στα θύματά του, χωρίς αυτό να γίνεται αντιληπτό. Οι τροποποιήσεις των μηνυμάτων μπορούν να πραγματοποιηθούν είτε σε πραγματικό χρόνο (*On-the-fly*) είτε αξιοποιούνται σε μελλοντική χρονική στιγμή για την πραγματοποίηση κάποιας επίθεσης αυτής της κατηγορίας.
- *Υποκλοπή Συνόδου (Session hijacking)*: Ο επιτιθέμενος σε αυτή την περίπτωση αξιοποιεί δεδομένα προηγούμενης έγκυρης συνόδου μεταξύ δύο οντοτήτων για τη μη εξουσιοδοτημένη πρόσβαση στους παρεχόμενους υπολογιστικούς πόρους και υπηρεσίες.
- *Επιθέσεις επανάληψης (Replay attacks)*: Ο επιτιθέμενος σε αυτή την περίπτωση, αφού έχει υποκλέψει κάποια από τα δεδομένα αυθεντικοποίησης, τα αξιοποιεί σε μεταγενέστερο χρόνο, για να επιτύχει πρόσβαση ως νόμιμος χρήστης, χωρίς βεβαίως να γίνεται αντιληπτό ότι δεν είναι πράγματι ο νόμιμος χρήστης.
- *Επιθέσεις πλαστοπροσωπίας (Impersonationn Attacks)*: Σε αυτές συμπεριλαμβάνονται οι περιπτώσεις όπου ο επιτιθέμενος έχει επιτύχει μη εξουσιοδοτημένη πρόσβαση σε κάποιο από τα διακριτικά αυθεντικοποίησης του νόμιμου χρήστη.
- *Επιθέσεις πλημμύρας (Flooding Attacks)*: Ο επιτιθέμενος προσπαθεί να δημιουργήσει σημαντικό υπολογιστικό φόρτο, κυρίως εξαιτίας των αυξημένων απαιτήσεων υπολογιστικών μεθόδων που αξιοποιούν τα πρωτόκολλα αυθεντικοποίησης και της μη ορθής διαχείρισης των υπολογιστικών πόρων του συστήματος που παρέχει την ηλεκτρονική υπηρεσία, με στόχο την ουσιαστικά αναίτια

κατανάλωση των υπολογιστικών πόρων του συστήματος για να προκαλέσει άρνηση παροχής υπηρεσίας (*Denial of Service*).

- *Επιθέσεις τροποποίησης δεδομένων (Data Modification Attacks):* Σε αυτή την περίπτωση πραγματοποιείται είτε επίθεση ενδιάμεσου, είτε περιλαμβάνεται η έγχυση κακόβουλου κώδικα (*Injection Attacks*) στα μεταδιδόμενα δεδομένα για τη μη εξουσιοδοτημένη τροποποίηση των αποθηκευμένων δεδομένων του συστήματος. Αντιπροσωπευτική επίθεση της τελευταίας περίπτωσης είναι η έγχυση (*Injection*) SQL κώδικα στα δεδομένα που αποστέλλει στην υπηρεσία με στόχο την τροποποίηση κάποιων αποθηκευμένων δεδομένων.
- *Επιθέσεις απόκρυψης ταυτότητας (Spoofing attacks)*: Ο επιτιθέμενος καθιστά εφικτή την απόκρυψη της αληθινής του ταυτότητας, αξιοποιώντας την ταυτότητα κάποιας άλλης εξουσιοδοτημένης οντότητας. Συγκεκριμένα, ο επιτιθέμενος χρησιμοποιεί μια πλαστή IP διεύθυνση, υπαρκτή ή μη, η οποία δεν αντιπροσωπεύει την πραγματική διεύθυνση των πακέτων που αποστέλλει, με στόχο την απόκρυψη της αρχικής πηγής της επίθεσης ή για να επιτύχει πρόσβαση σε μη εξουσιοδοτημένους πόρους.

Θα πρέπει να σημειωθεί ότι οι επιθέσεις-απειλές αυτές, διαφοροποιούνται στη διαδικασία εκτέλεσής τους, ανάλογα με την υπηρεσία ή το πρωτόκολλο αυθεντικοποίησης εναντίον των οποίων πραγματοποιείται η επίθεση.

3.4.4 Απειλές κατά τη Διαδικασία Εγγραφής Τελικού Χρήστη

Οι πιο γνωστές απειλές που εμφανίζονται κατά τη διαδικασία της εγγραφής (Burr et al., 2011) είναι οι ακόλουθες:

- *Πλαστοπροσωπία (Impersonation)*: Σε αυτή την περίπτωση ο αιτών ισχυρίζεται ψευδώς ότι είναι κάποια άλλη οντότητα και προσκομίζει ψευδή δικαιολογητικά προκειμένου να τεκμηριώσει τον ισχυρισμό του.
- *Αποποίηση Εγγραφής (Registration Repudiation)*: Ο αιτών προσπαθεί να αποποιηθεί την πεπραγμένη διαδικασία εγγραφής και τα συνθηματικά, ψηφιακά πιστοποιητικά που εκδόθηκαν ως συνέχεια αυτής.

3.4.5 Άλλες Απειλές

Επιπλέον των απειλών που παρουσιάζονται στις προηγούμενες ενότητες, τα υπολογιστικά συστήματα είναι ενδεχόμενο να αντιμετωπίσουν και τις ακόλουθες απειλές (Vivo et al., 1998):

- *Ιομορφικό λογισμικό (Viral Software)*: Το ιομορφικό λογισμικό περιλαμβάνει προγράμματα που σχεδιάζονται με σκοπό την εκτέλεση κακόβουλου κώδικα σε κάποιο υπολογιστικό σύστημα, χωρίς αυτό να γίνεται άμεσα αντιληπτό στο διαχειριστή του συστήματος, με σκοπό την εκδήλωση μιας επίθεσης. Το ιομορφικό λογισμικό κατηγοριοποιείται με βάση τις ιδιότητές του στα ακόλουθα:
- *Ιός (Virus)*: Ένας ιός αποτελεί ένα πρόγραμμα το οποίο έχει τη δυνατότητα να προστίθεται και να συνυπάρχει σε άλλο λογικό αντικείμενο, ενώ αναπαράγεται μέσω της ενεργοποίησης του λογικού αντικειμένου.
- *Δούρειος Ίππος (Trojan Horse)*: Ένας δούρειος ίππος είναι πρόγραμμα που συμπεριλαμβάνει κρυφές λειτουργίες, οι οποίες, όταν ενεργοποιηθούν, αξιοποιούν τα δικαιώματα του χρήστη που εκτελεί το δούρειο ίππο, και τις οποίες εκμεταλλεύονται οι επιτιθέμενοι, για να πραγματοποιήσουν μια επίθεση.
- *Σκουλήκια (Worms)*: Ένα σκουλήκι είναι ένα πρόγραμμα ιομορφικού λογισμικού, το οποίο έχει τη δυνατότητα να διαδίδεται και να αυτοαναπαράγεται.

Η μετάδοση του ιομορφικού λογισμικού σε κάποιο υπολογιστικό σύστημα μπορεί να πραγματοποιηθεί είτε με την αποθήκευσή του σε κάποιο μέσο αποθήκευσης είτε δικτυακά.

- *Υπερχειλίσεις προσωρινών χώρων (Buffer Overflow)*: Στις επιθέσεις υπερχείλισης προσωρινών χώρων, ο επιτιθέμενος εκμεταλλεύεται τον ελλιπή έλεγχο κατά την αποθήκευση των δεδομένων στους αντίστοιχους καταχωρητές, με αποτέλεσμα την τροποποίηση της ροής εκτέλεσης της εφαρμογής στην οποία πραγματοποιείται η επίθεση, με σκοπό την εκτέλεση του κώδικα που επιθυμεί ο επιτιθέμενος.
- *Μη εξουσιοδοτημένη είσοδος στο λειτουργικό σύστημα (Unauthorized Access)*. Ελλιπή συστήματα ελέγχου πρόσβασης στο λειτουργικό σύστημα ενδέχεται να επιτρέψουν σε ένα μη εξουσιοδοτημένο χρήστη, πρόσβαση σε εμπιστευτικές

πληροφορίες και εξουσιοδότηση για εκτέλεση ενεργειών τις οποίες κανονικά δε θα έπρεπε να εκτελέσουν.

3.5 Πιθανές Επιπτώσεις Απειλών – Κινδύνων

Οι απειλές που αναλύονται στην ενότητα 3.4, παρουσιάζουν διαφορετικές επιπτώσεις στους χρήστες και στους δημόσιους φορείς που προσφέρουν τις υπηρεσίες ηλεκτρονικής διακυβέρνησης, όταν αυτές αξιοποιηθούν σε μία επίθεση. Στον πίνακα που ακολουθεί αποτυπώνονται ενδεικτικά οι πιθανές επιπτώσεις που μπορεί να έχουν οι κίνδυνοι αυτοί, τόσο στους χρήστες όσο και στους δημόσιους φορείς σε σχέση με το επίπεδο εμπιστοσύνης που εντάσσεται η υπηρεσία. Θα πρέπει να σημειωθεί ότι ο πίνακας αυτός δεν αποτελεί πηγή εξαντλητικής αποτύπωσης των επιπτώσεων, καθώς αυτές διαφοροποιούνται ανάλογα με την εκάστοτε υπηρεσία και τις πιθανές επιπρόσθετες νομικές, οικονομικές κ.λπ. επιπτώσεις που ενδέχεται να υποστεί ο φορέας.

Κίνδυνος	**Πιθανές Επιπτώσεις Τελικών Χρηστών**	**Πιθανές Επιπτώσεις Φορέων Παροχής Υπηρεσιών**
Υποκλοπή Διακριτικών Αυθεντικοποίησης	Μη εξουσιοδοτημένη Πρόσβαση Παραβίαση Ιδιωτικότητας Υποβολή Λανθασμένων Στοιχείων	Επεξεργασία Λανθασμένων Στοιχείων
Επιθέσεις ενδιάμεσου	Παραβίαση Ιδιωτικότητας Υποβολή λανθασμένων στοιχείων	Επεξεργασία Λανθασμένων Στοιχείων Αντιποίηση Υπηρεσίας
Υποκλοπή Επικοινωνίας-Δεδομένων	Παραβίαση Ιδιωτικότητας Μη εξουσιοδοτημένη Πρόσβαση	Δημοσίευση Προσωπικών Δεδομένων
Υποκλοπή Συνόδου	Μη εξουσιοδοτημένη Πρόσβαση	Δημοσίευση Προσωπικών Δεδομένων
Επιθέσεις Επανάληψης	Μη εξουσιοδοτημένη Πρόσβαση Υποβολή λανθασμένων στοιχείων	Επεξεργασία Λανθασμένων Στοιχείων
Επιθέσεις Πλαστοπροσωπίας	Μη εξουσιοδοτημένη Πρόσβαση	Επεξεργασία Λανθασμένων Στοιχείων
Επιθέσεις Πλημμύρας	‘Άρνηση πρόσβασης στην Υπηρεσία	Μη Παροχή Υπηρεσίας
Επιθέσεις Τροποποίησης Δεδομένων	Υποβολή Λανθασμένων Στοιχείων	Επεξεργασία Λανθασμένων Στοιχείων
Ιομορφικό Λογισμικό	Άρνηση πρόσβασης στην Υπηρεσία	Μη Παροχή Υπηρεσίας

Κίνδυνος	Πιθανές Επιπτώσεις Τελικών Χρηστών	Πιθανές Επιπτώσεις Φορέων Παροχής Υπηρεσιών
Υπερχειλίσεις Προσωρινών Χώρων	Άρνηση πρόσβασης στην Υπηρεσία Μη εξουσιοδοτημένη Πρόσβαση	Μη Παροχής Υπηρεσίας Μη εξουσιοδοτημένη Πρόσβαση
Μη εξουσιοδοτημένη Είσοδος στο Λ.Σ.	Μη εξουσιοδοτημένη Πρόσβαση	Μη εξουσιοδοτημένη Πρόσβαση

Πίνακας 3-1: Κίνδυνοι και Πιθανές Επιπτώσεις

3.6 Τρόποι Αντιμετώπισης και Ελαχιστοποίησης Απειλών και Κινδύνων

Για την ελαχιστοποίηση της πιθανότητας μετουσίωσης μιας απειλής σε κίνδυνο, θα πρέπει τα μέτρα ασφάλειας τα οποία έχουν ληφθεί να αντιμετωπίζουν ικανοποιητικά τις τεθείσες απαιτήσεις ασφάλειας (*Security Requirements*) και, εφόσον απαιτείται, να περιλαμβάνουν, μεταξύ άλλων, την παροχή των ακολούθων υπηρεσιών ασφάλειας (*Security Services*):

- *Αυθεντικοποίηση (Authentication)*, η οποία σχετίζεται με το επίπεδο εμπιστοσύνης το οποίο οι συναλλασσόμενοι απαιτούν, σε σχέση με την ταυτότητα των εμπλεκομένων μερών.
- *Εξουσιοδότηση (Authorization)*, η οποία σχετίζεται με τα δικαιώματα που διαθέτει κάθε οντότητα, στο πλαίσιο μιας συναλλαγής.
- *Ακεραιότητα (Integrity)* των δεδομένων, που αφορά στην απαίτηση περί μη τροποποίησης του περιεχομένου των μηνυμάτων κατά τη διάρκεια μιας συναλλαγής.
- *Μη-αποποίηση (Non-repudiation)* αποστολής και λήψης δεδομένων, που αφορά στην παροχή στοιχείων, με βάση τα οποία μία οντότητα δε θα δύναται, κατ' αρχάς, σε μεταγενέστερο χρόνο να αρνηθεί ότι έχει συμμετάσχει σε μία συγκεκριμένη ηλεκτρονική συναλλαγή.
- Υπηρεσίες διασφάλισης της Εμπιστευτικότητας (*Confidentiality*) των ανταλλασσόμενων μηνυμάτων και γενικότερα της Ιδιωτικότητας (*Privacy*) των εμπλεκομένων οντοτήτων σε μία ηλεκτρονική συναλλαγή.

Στη συνέχεια περιγράφονται ενδεικτικές μέθοδοι για την αντιμετώπιση ή ελαχιστοποίηση των κινδύνων που αναφέρονται στην ενότητα 3.4.1 και παρουσιάζονται συγκεντρωτικά στον Πίνακας 3-2.

3.6.1 Ελαχιστοποίηση Απειλών Διακριτικών Αυθεντικοποίησης

Οι απειλές των διακριτικών αυθεντικοποίησης, όπως αυτές παρουσιάζονται στην ενότητα 3.4.2, κατηγοριοποιούνται με βάση τον τύπο του διακριτικού. Συνεπώς για την ελαχιστοποίηση εμφάνισης αυτού του είδους των απειλών θα πρέπει να ληφθούν τα αντίστοιχα προληπτικά μέτρα. Συγκεκριμένα, όσον αφορά στη διακύβευση των συνθηματικών του χρήστη, θα πρέπει να ακολουθούνται τα εξής:

- Αξιοποίηση Ασφαλών Συνθηματικών
- Ασφαλής αποθήκευσή τους και όχι σε μη κρυπτογραφημένη μορφή (*Clear Text*)
- Ασφαλής μετάδοση των διαπιστευτηρίων κατά τη διαδικασία αυθεντικοποίησης
- Περιορισμός έγκυρων προσπαθειών υποβολής συνθηματικού
- Τακτική αλλαγή του συνθηματικού από το χρήστη

Αντίστοιχα οι χρήστες οφείλουν να διατηρούν τα διακριτικά αυθεντικοποίησής τους σε ασφαλή μέρη ώστε να μην είναι δυνατή η υποκλοπή τους από κακόβουλους χρήστες

3.6.2 Ελαχιστοποίηση και Τρόποι αντιμετώπισης Απειλών στα Πρωτόκολλα Αυθεντικοποίησης και στις Παρεχόμενες Υπηρεσίες

Τα πρωτόκολλα αυθεντικοποίησης και οι ηλεκτρονικά παρεχόμενες υπηρεσίες αποτελούν τις βασικότερες ενότητες των υπηρεσιών ηλεκτρονικής διακυβέρνησης. Συνεπώς, η ελαχιστοποίηση εμφάνισης των κινδύνων, αλλά και η πιθανή αντιμετώπισή τους, συμβάλλουν στη διασφάλιση της ορθής λειτουργίας των συστημάτων αυτών (Evangelidis, 2004) . Για το λόγο αυτό, για κάθε κίνδυνο που παρουσιάστηκε στην ενότητα 3.4.3 θα πρέπει να λαμβάνονται τα αντίστοιχα μέτρα ελαχιστοποίησης και αντιμετώπισης. Συγκεκριμένα:

- *Υποκλοπή επικοινωνίας-δεδομένων*: Τα πρωτόκολλα αυθεντικοποίησης και οι παρεχόμενες ηλεκτρονικά υπηρεσίες θα πρέπει να διασφαλίζουν την εμπιστευτικότητα των κρίσιμων δεδομένων όπως συνθηματικά, μυστικά κλειδιά που σχετίζονται με τη διαδικασία αυθεντικοποίησης, και τα ευαίσθητα δεδομένα που ανταλλάσσονται και επεξεργάζονται από αυτές. Αυτό σημαίνει ότι ο επιτι-

θέμενος που καταγράφει υποκλέπτοντας την επικοινωνία, δεν είναι δυνατό να αποκαλύψει οποιοδήποτε πληροφορία που να τον οδηγεί στη διακύβευση εμπιστευτικών πληροφοριών, είτε σχετίζονται με τα διαπιστευτήρια του χρήστη, είτε με ευαίσθητες πληροφορίες που αφορούν τον ίδιο. Για το λόγο αυτό τα δεδομένα που σχετίζονται με τα πρωτόκολλα αυθεντικοποίησης και τις υπηρεσίες, τουλάχιστον όσον αφορά στις κρίσιμες πληροφορίες-δεδομένα, δε θα πρέπει να μεταδίδονται σε καθαρή μη-κρυπτογραφημένη μορφή, αλλά θα πρέπει να αξιοποιούν κατάλληλους μηχανισμούς ασφάλειας, ώστε να διασφαλίζεται η εμπιστευτικότητά τους.

- *Επιθέσεις Ενδιάμεσου*: Η ελαχιστοποίηση της πιθανότητας εμφάνισης αυτού του είδους των επιθέσεων μπορεί να πραγματοποιηθεί μόνο με την αξιοποίηση μηχανισμών ασφάλειας, όπως για παράδειγμα το πρωτόκολλο SSL, το οποίο στοχεύει και στην προστασία από τέτοιου είδους επιθέσεις ή άλλων εναλλακτικών συστημάτων αυθεντικοποίησης (Jun et al., 2006), που έχει αποδειχθεί η ρωμαλεότητα (*Robustness*) τους σε επιθέσεις ενδιάμεσου. Παρά ταύτα θα πρέπει να σημειωθεί ότι, ακόμα και σε αυτές τις περιπτώσεις, υπάρχουν περιπτώσεις πραγματοποίησης τέτοιου είδους επιθέσεων (NZ eGov, 2009).
- *Επιθέσεις Επανάληψης και Υποκλοπής Συνόδων*: Για την αποφυγή τέτοιους είδους επιθέσεων, τα πρωτόκολλα αυθεντικοποίησης και οι παρεχόμενες υπηρεσίες δε θα πρέπει να επεξεργάζονται δεδομένα που σχετίζονται με προηγούμενες συνόδους και που είναι δυνατό να επηρεάσουν την ορθή λειτουργία του συστήματος. Επιπλέον, θα πρέπει να επισημανθεί ότι, όπως και στις περιπτώσεις υποκλοπών δεδομένων, τα δεδομένα που μπορούν να οδηγήσουν σε διακύβευση της ασφάλειας του συστήματος είτε με επίθεση επανάληψης είτε με υποκλοπή συνόδου, δεν θα πρέπει να μεταδίδονται σε μη κρυπτογραφημένη μορφή, αλλά θα πρέπει να αξιοποιούνται οι κατάλληλοι μηχανισμοί ασφάλειας, ώστε να διασφαλίζεται η εμπιστευτικότητα τους.
- *Επιθέσεις Πλαστοπροσωπίας*: Στις επιθέσεις πλαστοπροσωπίας ο επιτιθέμενος προσπαθεί να αποδείξει την κατοχή νόμιμων διαπιστευτηρίων. Για το λόγο αυτό, τα πρωτόκολλα αυθεντικοποίησης δε θα πρέπει να αποκαλύπτουν δεδομένα που μπορεί να οδηγήσουν στην επίτευξη επιθέσεων πλαστοπροσωπίας.

- *Επιθέσεις Πλημμύρας*: Οι επιθέσεις πλημμύρας, τόσο στα πρωτόκολλα αυθεντικοποίησης όσο και στις παρεχόμενες υπηρεσίες, είναι σχετικά δύσκολο να ελαχιστοποιηθούν, αλλά μπορούν να ανιχνευθούν και να αντιμετωπισθούν στη συνέχεια με την αξιοποίηση κατάλληλων μηχανισμών.
- *Επιθέσεις Τροποποίησης Δεδομένων*: Οι επιθέσεις τροποποίησης δεδομένων τόσο στα πρωτόκολλα αυθεντικοποίησης όσο και στις παρεχόμενες υπηρεσίες, μπορούν να αντιμετωπισθούν με την αξιοποίηση κατάλληλων μηχανισμών ακεραιότητας, όπως message authentication code ή message integrity checksum, H-MAC και ψηφιακές υπογραφές (Ferguson & Schneier, 2003).
- *Επιθέσεις Απόκρυψης Ταυτότητας (Spoofing)*: Οι επιθέσεις αυτές μπορούν να ελαχιστοποιηθούν με την αξιοποίηση κατάλληλων μηχανισμών φιλτραρίσματος (*Ingress filtering*) (Γκρίτζαλης et al., 2003), οι οποίοι δεν επιτρέπουν την κίνηση δεδομένων σε συγκεκριμένα τμήματα ενός συγκεκριμένου δικτύου. Ο μηχανισμός αυτός μπορεί να εφαρμοστεί σε οποιοδήποτε ανάχωμα ασφαλείας (*Firewall*) επιπέδου δικτύου υλοποιεί τη μέθοδο που περιγράφεται στο RFC 2267.

3.6.3 Ελαχιστοποίηση και Τρόποι Αντιμετώπισης των Απειλών κατά τη Διαδικασία Εγγραφής Τελικού Χρήστη

Σε αρκετές περιπτώσεις οι απειλές της ενότητας 3.4.4 οφείλονται στις επιθέσεις που μπορούν να πραγματοποιηθούν κατά τη διαδικασία εγγραφής. Για το λόγο αυτό, η υπηρεσία εγγραφής θα πρέπει να:

- Ταυτοποιεί και να αυθεντικοποιεί τις οντότητες που αιτούνται εγγραφής σε κάποια υπηρεσία,
- Είναι αυστηρή και ακριβής κατά τον έλεγχο της ορθότητας των υποβληθέντων δικαιολογητικών και στοιχείων, ώστε να είναι δυνατή η ανίχνευση ψευδών δικαιολογητικών και να
- Αξιοποιεί διαδικασίες καταγραφής όλων των ενεργειών που πραγματοποιούνται από την υπηρεσία εγγραφής, ώστε να μην είναι δυνατή η αποποίηση εγγραφής σε κάποια υπηρεσία από μια οντότητα.

3.6.4 Ελαχιστοποίηση και Τρόποι Αντιμετώπισης Άλλων Απειλών

Σε αρκετές περιπτώσεις, οι απειλές που αναφέρονται στις ενότητες 3.4.1, 3.4.2, 3.4.3, εκδηλώνονται εκμεταλλευόμενες κάποια αδυναμία που προκαλείται ως συνέπεια της εκδήλωσης κάποιας άλλης γενικής απειλής (ενότητα 3.4.4). Για το λόγο αυτό θα πρέπει οι γενικές αυτές απειλές να ελαχιστοποιούνται και να αντιμετωπίζονται άμεσα. Αυτό συνεπάγεται ότι οι διαχειριστές των υπολογιστικών συστημάτων πρέπει να ενημερώνουν άμεσα τα συστήματα που διαχειρίζονται, με τις νέες εκδόσεις (*Version*) λογισμικού, τουλάχιστον αυτών που σχετίζονται με την ασφάλεια και τη διαθεσιμότητα των υπολογιστικών συστημάτων (πακέτα αναβάθμισης λογισμικού (*Patches*), ενημερώσεις ιών κτλ).

Απειλή		**Τρόποι αντιμετώπισης**
Απειλές Διακριτικών Αυθεντικοποίησης	Υποκλοπή δεδομένων που γνωρίζει ο χρήστης (π.χ. συνθηματικού) με: • Επιθέσεις λεξικών • Επιθέσεις εξαντλητικής αναζήτησης • Επιθέσεις τυχαίων δοκιμών • Υποκλοπή κατά τη μετάδοση των διαπιστευτηρίων	• Αξιοποίηση Ασφαλών Συνθηματικών • Ασφαλή αποθήκευση τους και όχι σε καθαρή μορφή • Ασφαλή μετάδοση των διαπιστευτηρίων κατά τη διαδικασία αυθεντικοποίησης • Περιορισμός έγκυρων προσπαθειών υποβολής συνθηματικού
	Υποκλοπή δεδομένων που έχει υπό την κατοχή του ο χρήστης με σκοπό την αντιγραφή ή τη χρησιμοποίηση σε κάποια δοσοληψία χωρίς τη γνώση του (π.χ. ιδιωτικό κλειδί)	Διατήρηση των διακριτικών αποθήκευσης σε ασφαλή μέρη ώστε να μην είναι δυνατή η υποκλοπή του από κακόβουλους χρήστες.
Απειλές στα Πρωτόκολλα Αυθεντικοποίησης & στις Παρεχόμενες υπηρεσίες	Υποκλοπή επικοινωνίας-δεδομένων (*Eavesdropping*): • Υποκλοπή δεδομένων • Ανάλυση των δεδομένων (*Traffic analysis*) και αξιοποίηση τους σε μελλοντική επίθεση	Τα δεδομένα δε θα πρέπει να μεταδίδονται σε καθαρή μορφή (clear text) αλλά θα πρέπει να αξιοποιούν κατάλληλους μηχανισμούς ασφάλειας ώστε να διασφαλίζεται η εμπιστευτικότητα των δεδομένων αυτών.
	Επιθέσεις ενδιάμεσου (*Man-in-the-middle attacks*)	Αξιοποίηση ισχυρών μηχανισμών ασφάλειας

Απειλή		Τρόποι αντιμετώπισης
	Επιθέσεις επανάληψης (*Replay attacks*)	Δε θα πρέπει να γίνεται επεξεργασία δεδομένων που σχετίζονται με προηγούμενες συνόδους και μπορούν να επηρεάσουν την ορθή λειτουργία του συστήματος
	Υποκλοπή Συνόδου (*Session Hijacking*)	
	Επιθέσεις πλαστοπροσωπίας (*Impersonation Attacks*)	Τα πρωτόκολλα αυθεντικοποίησης δε θα πρέπει να αποκαλύπτουν οποιαδήποτε δεδομένα που μπορεί να οδηγήσουν στην επίτευξη επιθέσεων πλαστοπροσωπίας
	Επιθέσεις πλημμύρας (*Flooding attacks*)	Αξιοποίηση κατάλληλων μηχανισμών ανίχνευσης επιθέσεων πλημμύρας
	Επιθέσεις Τροποποίησης Δεδομένων (*Data Modification Attacks*)	Αξιοποίηση κατάλληλων μηχανισμών ακεραιότητας
	Spoofing	Αξιοποίηση κατάλληλων μηχανισμών οι οποίοι δεν επιτρέπουν την κίνηση δεδομένων σε συγκεκριμένα τμήματα του δικτύου
Απειλές κατά τη διαδικασία εγγραφής	Πλαστοπροσωπία (*Impersonation*)	Αξιοποίηση κατάλληλων μηχανισμών ταυτοποίησης
	Αποποίηση Εγγραφής (*Registration Repudiation*)	Αξιοποίηση μηχανισμών μη-αποποίησης (*Non-repudiation*)
Άλλες Απειλές	Ιομορφικό λογισμικό (*Viral software*): • Ιός (*Virus*) • Δούρειος Ίππος (*Trojan horse*) • Σκουλήκια (*Worms*)	Άμεση ενημέρωση των υπολογιστών με τις νέες εκδοχές, τουλάχιστον σε ότι σχετίζεται με την ασφάλεια των υπολογιστικών συστημάτων (patches, ενημερώσεις ιών κτλ).
	Υπερχειλίσεις Προσωρινών Χώρων (B*uffer overflow*)	

Απειλή		Τρόποι αντιμετώπισης
	Μη εξουσιοδοτημένη είσοδος στο λειτουργικό σύστημα	

Πίνακας 3-2: Πιθανές Απειλές και Τρόποι Αντιμετώπισης

3.6.5 Ανάλυση Επικινδυνότητας και Αποτίμηση Κινδύνου

Τα περιουσιακά στοιχεία (*Assets*) ενός Π.Σ. Ηλεκτρονικής Διακυβέρνησης τα οποία πρέπει να προστατευτούν είναι τα εξής:

- Υλικό (*Hardware*),
- Λογισμικό (*Software*),
- Πληροφορίες και Δεδομένα (*Information and Data*),
- Τεκμηρίωση διαδικασιών (*Procedure Documentation*),
- Προσωπικό (*Personne*l) και
- Εγκαταστάσεις (*Facilities*).

Η αξία των αγαθών προσδιορίζεται με διαφορετικό τρόπο ανάλογα με τη φύση του αγαθού. Για παράδειγμα, η αξία του υλικού ή άλλου εξοπλισμού μπορεί να υπολογιστεί σε σχέση με το οικονομικό μέγεθος που θα απαιτηθεί για την αντικατάστασή της. Αντίθετα, η αξία των αγαθών μπορεί να υπολογιστεί σε σχέση με τις επιπτώσεις απώλειας της ασφάλειάς τους, δηλαδή σε σχέση με ενδεχόμενη παραβίαση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητάς τους καθώς και σε σχέση με τις επιπτώσεις από την παραβίαση αυτή. Απειλή (*Threat*) είναι οποιαδήποτε πράξη ή γεγονός που θα μπορούσε ενδεχομένως να έχει επιβλαβές (*Harmful*) αποτέλεσμα στο Π.Σ. Παραδείγματα τέτοιων απειλών είναι:

- Φυσικές απειλές (π.χ. φωτιά),
- Φυσικές καταστροφές (π.χ. σεισμός),
- Απώλεια υπηρεσιών (π.χ. διακοπή ηλεκτροδότησης),
- Καταστροφή δεδομένων,
- Τροποποίηση δεδομένων,
- Παρακολούθηση δεδομένων,
- Σφάλματα (π.χ. σφάλμα εξυπηρετητή ή λογισμικού) και
- Μη εξουσιοδοτημένες ενέργειες (π.χ. μη εξουσιοδοτημένη χρήση εξοπλισμού)

Ως ευπάθεια (*Vulnerability*) ορίζεται μια αδυναμία του Π.Σ., η ύπαρξη της οποίας μπορεί να επιτρέψει την πραγματοποίησης μιας απειλής. Παραδείγματα ευπαθειών είναι:

- Ευπάθειες υλικού (π.χ. έλλειψη σωστών πρακτικών απόσυρσης υλικού),
- Ευπάθειες λογισμικού (π.χ. παράλειψη αποσύνδεσης χρηστών),
- Ευπάθειες δικτύου (π.χ. μη κρυπτογραφημένη μετάδοση εμπιστευτικών πληροφοριών),
- Ευπάθειες προσωπικού (π.χ. έλλειψη ενημερότητας ασφάλειας) και
- Ευπάθειες διοίκησης (π.χ. έλλειψη τεκμηριωμένων διαδικασιών)

Επίπτωση είναι το αποτέλεσμα της αποτυχίας να διαφυλαχθεί η ασφάλεια του Π.Σ., δηλαδή το αποτέλεσμα από μία επιτυχημένη παραβίαση της ασφάλειάς του. Οι επιπτώσεις που μπορεί να προκύψουν από μία τέτοια παραβίαση κατηγοριοποιούνται σε 4 βασικούς τύπους:

- Διαρροή (*Leak*),
- Τροποποίηση (*Modification*),
- Καταστροφή (*Destruction*) και
- Μη διαθεσιμότητα (*Unavailability*)

Μετά τον υπολογισμό της επικινδυνότητας έπεται η επιλογή και εφαρμογή αντιμέτρων (*Countermeasures*) για τη διασφάλιση – προστασία του Π.Σ. Ως αντίμετρο νοείται ένα μηχανισμός ή μια διαδικασία που λειτουργεί στο περιβάλλον του Π.Σ. με σκοπό να ελαττώσει ένα ή περισσότερα από τα συστατικά της επικινδυνότητας στην οποία είναι εκτεθειμένο. Τα πιθανά αντίμετρα κατηγοριοποιούνται σε 4 βασικούς τύπους:

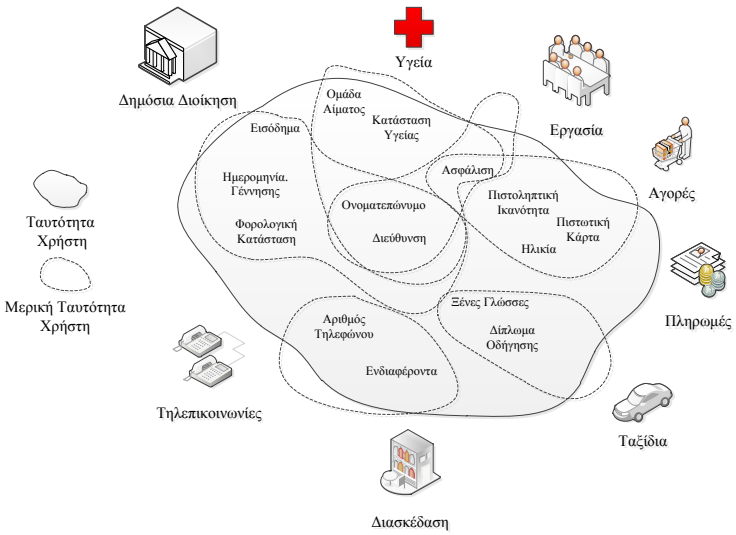
- Φυσικά (*Physical*),
- Διαδικαστικά (*Procedural*),
- Τεχνικά (*Technical*) και
- Προσωπικού (*Personnel*).

ΚΕΦΑΛΑΙΟ 4 - ΨΗΦΙΑΚΑ ΑΝΑΓΝΩΡΙΣΤΙΚΑ

Στο παρόν κεφάλαιο αναλύεται διεξοδικά η συσχέτιση της πραγματικής ταυτότητας του τελικού χρήστη με την ψηφιακή του ταυτότητα, τα συστήματα διαχείρισής της καθώς και οι διαφορετικές πρακτικές-μεθοδολογίες ταυτοποίησης και διασύνδεσης μερικών ψηφιακών ταυτοτήτων. Επιπρόσθετα προτείνονται μεθοδολογίες για την αποθήκευση πολλαπλών αναγνωριστικών σε ψηφιακά πιστοποιητικά X.509 v3, ενσωμάτωσης και διαχείρισης τομεακών αναγνωριστικών τελικών χρηστών σε περιβάλλοντα ομόσπονδων ταυτοτήτων καθώς και σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης 2.0, ενώ αποτυπώνονται και οι προκλήσεις διαχείρισης των ψηφιακών ταυτοτήτων σε νεφοϋπολογιστικά συστήματα Ηλεκτρονικής Διακυβέρνησης.

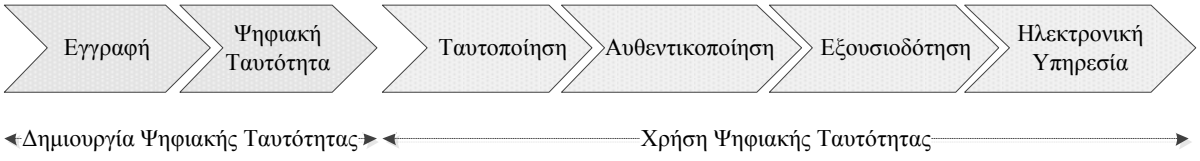
4.1 Ψηφιακή Ταυτότητα

Στο φυσικό κόσμο, η ταυτότητα κάθε ατόμου αποτελείται από μια μεγάλη ποικιλία χαρακτηριστικών και γνωρισμάτων ικανών να τον αναγνωρίσουν μοναδικά είτε μόνα τους, είτε σε συνδυασμό μεταξύ τους (Buell & Sandhu, 2003). Ανάλογα την περίπτωση, το πλαίσιο (context) και το ρόλο (role) που θέλει να αναλάβει το συγκεκριμένο άτομο, επιλέγει να χρησιμοποιήσει και να αποκαλύψει κάποιο υποσύνολο της ταυτότητάς τους, το οποίο αποτελεί μία μερική ταυτότητα (Clauß & Köhntopp, 2001). Το σύνολο των μερικών ταυτοτήτων αποτελούν την ταυτότητα του κάθε ατόμου, όπως απεικονίζονται και στο Σχήμα 4-1. Η ραγδαία ανάπτυξη και διάδοση των τεχνολογιών Διαδικτύου και των καινούργιων μηχανισμών ολοκλήρωσης των παραδοσιακών συναλλαγών ηλεκτρονικά, εισήγαγε την έννοια της ψηφιακής ταυτότητας (Corradini et al., 2007). Υπό τη στενή έννοια του όρου, όπως αυτή γίνεται αντιληπτή από τα Π.Σ., αυτή νοείται ως "*ηλεκτρονικά αναγνωρίσιμη αντιπροσώπευση μιας ανθρώπινης ταυτότητας*" (Camp, 2004). Σκοπός της είναι να συνδέσει μία συγκεκριμένη συναλλαγή ή ένα σύνολο δεδομένων από ένα Π.Σ. με ένα αναγνωρίσιμο άτομο. Η χρήση της επιτρέπει την ταυτοποίηση και εξουσιοδότηση του συγκεκριμένου ατόμου για τη χρήση υπολογιστικών πόρων ή ηλεκτρονικών υπηρεσιών.



Σχήμα 4-1: Ταυτότητα - Μερικές Ταυτότητες Ατόμου (Clauß & Köhntopp, 2001)

Στο πλαίσιο των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, οι συγκεκριμένοι πόροι μπορεί να αφορούν υπηρεσίες είτε προς τους πολίτες (*G2C*) είτε προς τις επιχειρήσεις (*G2B*). Προκειμένου να δοθεί πρόσβαση σε κάποιον χρήστη για μία συγκεκριμένη ηλεκτρονική υπηρεσία, θα πρέπει να προηγηθούν αρκετά στάδια επεξεργασίας. Το πρώτο στάδιο περιλαμβάνει τη δημιουργία της ψηφιακής ταυτότητας του χρήστη που μπορεί να αποτελείται από έναν συνδυασμό ονόματος χρήστη (*Username*) και συνθηματικού (*Password*), ένα ψηφιακό πιστοποιητικό (*Digital Certificate*) ή ένα ανώνυμο διακριτικό διαπιστευτήριο (*Anonymous*). Προτού ολοκληρωθεί η διαδικασία δημιουργίας, θα πρέπει να προηγηθεί η διαδικασία της εγγραφής (*Registration*), κατά την οποία ο εκδότης της ψηφιακής ταυτότητας ελέγχει, αν αυτή εκδίδεται για το σωστό πρόσωπο, αν πληροί όλες τις προϋποθέσεις και αν δικαιούται τη συγκεκριμένη μορφή ψηφιακής ταυτότητας. Στο Σχήμα 4-2 που ακολουθεί, απεικονίζονται τα στάδια από την δημιουργία έως τη χρήση της ηλεκτρονικής υπηρεσίας.



Σχήμα 4-2: Ψηφιακή Ταυτότητα Χρήστη για Αξιοποίηση Ηλεκτρονικής Υπηρεσίας

Τα στάδια που περιλαμβάνονται στη χρήση της ηλεκτρονικής υπηρεσίας και αφορούν τον έλεγχο πρόσβασης του χρήστη (*Access Control*), είναι τα:

- *Ταυτοποίηση (Identification)*: Ο χρήστης ισχυρίζεται την ύπαρξη συγκεκριμένης ψηφιακής ταυτότητας, παρέχοντας π.χ. ένα όνομα χρήστη
- *Αυθεντικοποίηση (Authentication)*: Ο χρήστης επαληθεύει την ύπαρξη της προαναφερθείσας ψηφιακής ταυτότητας παρέχοντας π.χ. ένα συνθηματικό και ο συνδυασμός τους επαληθεύεται από τον πάροχο της ηλεκτρονικής υπηρεσίας
- *Εξουσιοδότηση (Authorization):* Ο πάροχος προσδιορίζει τα δικαιώματα του χρήστη για τη συγκεκριμένη ηλεκτρονική υπηρεσία

4.2 Ηλεκτρονική Διαχείριση Ψηφιακής Ταυτότητας

Οι βασικότεροι ορισμοί που αποδίδονται στον όρο Ηλεκτρονική Διαχείρισης Ταυτότητας (*electronic Identity Management*) είναι "*το σύνολο των διαδικασιών που επιτρέπουν την δημιουργία, διατήρηση και κατάργηση των πληροφοριών που ορίζουν μοναδικά κάθε χρήστη ενός συνόλου πληροφοριακών συστημάτων*" (Rosenberg, 1992) και "*το σύνολο των διαδικασιών, εργαλείων και κοινωνικών συμβολαίων που προσδιορίζουν την δημιουργία, διατήρηση και κατάργηση της ψηφιακής ταυτότητας ατόμων για την ασφαλή πρόσβαση σ' ένα διευρυνόμενο σύνολο συστημάτων και εφαρμογών*" (Pato, 2003). Τα κύρια σημεία των δύο αυτών ορισμών, σύμφωνα και με (Πουλούδη et al., 2007), είναι:

- Ο προσδιορισμός των επιχειρηματικών διαδικασιών που απαιτούν ταυτοποίηση των χρηστών,
- Ο βαθμός απαίτησης για την ταυτοποίηση των χρηστών, το πόσο ισχυρή είναι η ταυτότητα που δημιουργείται από το σύστημα και αν είναι ανθεκτική σε αντιγραφή ή κακή χρήση της,
- Η διακριτική προσπέλαση των χρηστών σε διάφορες υπηρεσίες και
- Η επιλογή εκείνων των εργαλείων που θα διαχειρίζονται αποτελεσματικά τις ταυτότητες των χρηστών και θα δημιουργούν ένα ασφαλές περιβάλλον χωρίς προβλήματα

Τα συστήματα διαχείρισης ταυτότητας απαρτίζονται από μια σειρά υπηρεσιών και επιμέρους συστημάτων, τα οποία έχουν ως στόχο μια συνολική αντιμετώπιση της έκδοσης, διαχείρισης και κατάργησης των δεδομένων που συγκροτούν την ταυτότητα των χρηστών. Τα επιμέρους στοιχεία ενός τυπικού συστήματος διαχείρισης ταυτότητας περιγράφονται από τον (Pato, 2003).

Σχήμα 4-3: Βασικά Τμήματα Συστημάτων Ηλεκτρονικής Διαχείρισης Ταυτοτήτων (Pato, 2003)

Στο επίκεντρο κάθε συστήματος διαχείρισης ταυτότητας βρίσκεται το Ψηφιακό Αποθετήριο (*Data Digital Repository*), όπου αποθηκεύονται τα δεδομένα του συστήματος (*Logical data*), και το Μοντέλο δεδομένων ταυτότητας (*Identity data model*). Επιπλέον, στο τμήμα αυτό αποθηκεύονται και οι κανόνες που ορίζουν την πρόσβαση και διαχείριση της πληροφορίας. Το σύστημα διαχείρισης ταυτότητας διαρθρώνεται σε τρία επίπεδα. Κάθε ένα από αυτά τα επίπεδα αποσκοπεί στη ρύθμιση εκείνων των στοιχείων που σχετίζονται με τους κανόνες δημιουργίας και διαχείρισης των δεδομένων και την πρόσβαση στο σύστημα των κατόχων αυτών. Τα επίπεδα αυτά, σύμφωνα με (Pato, 2003) και (Πουλούδη et al., 2007), είναι:

- *Βάση (Foundation)*: πρόκειται για το επίπεδο που ρυθμίζει τους κανόνες πρόσβασης στα δεδομένα που τηρούνται στο σύστημα
- *Κύκλος ζωής (Lifecycle)*: εδώ ρυθμίζονται όλα εκείνα στοιχεία που αφορούν στην έκδοση ηλεκτρονικών ταυτοτήτων, καθώς και στη διαχείριση των δεδομένων που τις απαρτίζουν
- *Πρόσβαση & χρήση (Consumable)*: στο επίπεδο αυτό ορίζεται ο τρόπος πρόσβασης και προσπέλασης των δεδομένων στο σύστημα.

Σε κάθε ένα από αυτά τα επίπεδα, διάφορα τμήματα του συστήματος ταυτότητας αλληλεπιδρούν, με στόχο τη συλλογή και αποτελεσματική διαχείριση των δεδομένων, που θα επιτρέψει την απρόσκοπτη χρήση των υπηρεσιών του από τον τελικό χρήστη.

Η βάση ενός συστήματος διαχείρισης ταυτότητας, σύμφωνα πάλι με (Pato, 2003), αποτελείται από τα εξής μέρη:

- *Πάροχος Αυθεντικοποίησης (Authentication Provider):* είναι υπεύθυνος για την αρχική αυθεντικοποίηση κάθε οντότητας που θα συνδεθεί με συγκεκριμένη ψηφιακή ταυτότητα. Παράγει ένα διακριτικό αυθεντικοποίησης (*Token Authenticator*), που επιτρέπει στις υπόλοιπες συνιστώσες του συστήματος (components) να γνωρίζουν ότι η αρχική αυθεντικοποίηση έχει ολοκληρωθεί επιτυχώς. Αυτές οι τεχνικές περιλαμβάνουν μηχανισμούς, όπως επαλήθευση συνθηματικών, επαλήθευση διακριτικών έξυπνων καρτών (*Smart Cards*), σαρώσεις βιομετρικών δεδομένων κ.α. Κάθε ταυτότητα μπορεί να σχετίζεται με περισσότερους από έναν παρόχους αυθεντικοποίησης. Οι μηχανισμοί που χρησιμοποιούνται από τον κάθε πάροχο, διαφέρουν ως προς την αποτελεσματικότητα και την ασφάλειά τους. Έτσι, ανάλογα με το πλαίσιο χρήσης ενός συστήματος διαχείρισης ταυτότητας, είναι δυνατόν να απαιτούνται συγκεκριμένοι μηχανισμοί αυθεντικοποίησης.
- *Έλεγχος Πολιτικής (Policy Control):* Η πρόσβαση και χρήση των δεδομένων και πληροφοριών που σχετίζονται με την ηλεκτρονική ταυτότητα, διέπεται από μια σειρά κανόνων. Οι πολιτικές εξουσιοδότησης προσδιορίζουν τον τρόπο διαχείρισης, διαχείρισης και εκχώρησης της πληροφορίας. Έλεγχοι αυτών των πολιτικών μπορεί να εγείρουν ελέγχους σε συγκεκριμένα περιστατικά (*Events*), καθώς και να ενημερώσουν το υποκείμενο της ταυτότητας για προσπέλαση των δεδομένων του.
- *Έλεγχος (Auditing):* Οι διαδικασίες ελέγχου αποτελούν το μηχανισμό επίβλεψης για τον τρόπο με τον οποίο η πληροφορία δημιουργείται, μεταβάλλεται και χρησιμοποιείται. Με αυτό τον τρόπο καθίσταται δυνατός ο εντοπισμός περιπτώσεων παραβίασης των πολιτικών του συστήματος.

Τα συστατικά του κύκλου ζωής ενός συστήματος διαχείρισης ταυτότητας είναι τα εξής:

- *Παροχή (Provisioning)*: Αφορά την αυτοματοποίηση όλων των διαδικασιών και των εργαλείων διαχείρισης του κύκλου ζωής μιας ταυτότητας και περιλαμβάνει τη δημιουργία ενός αναγνωριστικού (*Identifier*) για την ψηφιακή ταυτότητα, τη διασύνδεση με τους παρόχους αυθεντικοποίησης, τον προσδιορισμό και τη με-

ταβολή των χαρακτηριστικών αλλά και των προνομίων καθώς και την κατάργηση της ταυτότητας.

- *Διάρκεια (Longevity)*: Αφορά τη δημιουργία εγγραφών ιστορικού κάθε διακριτής ταυτότητας, καθώς και την εξέλιξη και διαφοροποίησή της με την πάροδο του χρόνου.

Το επίπεδο πρόσβασης και χρήσης του συστήματος περιλαμβάνει τα ακόλουθα στοιχεία:

- *Ενιαία πρόσβαση (Single Sign-On)*: με τον τρόπο αυτό η ταυτότητα του χρήστη πιστοποιείται μια φορά κατά την πρόσβασή του σε μια υπηρεσία του συστήματος ταυτότητας. Στη συνέχεια, μπορεί να έχει πρόσβαση σε όλες τις υπηρεσίες και τα συστήματα που έχουν διασυνδεθεί και απαρτίζουν το ευρύτερο περιβάλλον που διαχειρίζεται το σύστημα διαχείρισης ταυτότητας.
- *Εξατομίκευση (Personalization)*: τα εργαλεία αυτά επιτρέπουν, πληροφορίες που αφορούν στις εφαρμογές που χρησιμοποιεί ο χρήστης, καθώς και γενικές πληροφορίες να διασυνδεθούν με μια συγκεκριμένη ταυτότητα. Αυτά τα εργαλεία επιτρέπουν αφενός στον χρήστη να έχει μια εμπειρία, κατά την χρήση του συστήματος, προσαρμοσμένη στις προτιμήσεις του. Αφετέρου, επιτρέπουν στις επιχειρήσεις που διαχειρίζονται το σύστημα, να συγκεντρώνουν χρήσιμες πληροφορίες που μπορούν στη συνέχεια να χρησιμοποιήσουν για εμπορικούς σκοπούς.
- *Διαχείριση Πρόσβασης (Access Management)*: Επιτρέπει την πρόσβαση στους πόρους του συστήματος με βάση τα δικαιώματα και τους κανόνες που έχουν αποθηκευτεί στο αποθετήριο.

4.3 Θέματα Διαχείρισης Ταυτότητας σε Περιβάλλοντα ΗΔ

Συνήθη θέματα που σχετίζονται με την έννοια της ταυτότητας στο ηλεκτρονικό περιβάλλον, και συγκεκριμένα στο Διαδίκτυο (Πουλούδη et al., 2007), (Stefanova et al., 2010), είναι τα παρακάτω:

- αυξημένη ανάγκη ταυτοποίησης των συναλλασσομένων
- επιθυμία των χρηστών να διατηρήσουν τις συνήθειες του «πραγματικού» κόσμου δηλαδή να διατηρούν την ανωνυμία τους στις συναλλαγές

- επικράτηση μιας κουλτούρας, όπου ο κάθε χρήστης, όχι μόνο δεν αποκαλύπτει την ταυτότητά του κατά την περιήγησή του στο Διαδίκτυο, αλλά χρησιμοποιεί ένα ή περισσότερα ψευδώνυμα
- δυνατότητα εταιρειών να συλλέξουν σημαντικές πληροφορίες για τις συνήθειες των συναλλασσομένων.

Στο πλαίσιο της Ηλεκτρονικής Διακυβέρνησης, το ζήτημα της ηλεκτρονικής διαχείρισης ταυτότητας (*electronic Identity Management - eIdM*) είναι σαφώς πιο έντονο σε σχέση με τη μέχρι σήμερα σημασία του στις εμπορικές συναλλαγές, καθώς αποτελεί βασικό παράγοντα και προϋπόθεση για την ασφαλή και αποτελεσματική χρήση ηλεκτρονικών υπηρεσιών και συναλλαγών. Οι βασικές ανησυχίες των πολιτών αφορούν κυρίως στα δεδομένα που το κάθε κράτος επιλέγει να απαρτίζουν την πληροφοριακή τους ταυτότητα (*Informational Identity*). Στο ηλεκτρονικό εμπόριο, η ψηφιακή ταυτότητα του ατόμου διαμορφώνεται εν μέρει με τη δική του συμβολή. Στην Ηλεκτρονική Διακυβέρνηση κάτι τέτοιο δεν είναι εφικτό, αφού η Δημόσια Διοίκηση είναι αυτή που προσδιορίζει τις πληροφοριακές ανάγκες. Οι ανησυχίες που εγείρει η διαχείριση ταυτότητας στο πλαίσιο της Ηλεκτρονικής Διακυβέρνησης, σχετίζονται κυρίως με τους φορείς ταυτοποίησης και αυθεντικοποίησης, οι οποίοι συγκεντρώνουν ευαίσθητα και μοναδικά στοιχεία του ατόμου, για τα οποία, μέχρι πρότινος, φορέας διαχείρισης ήταν το ίδιο το άτομο (Πουλούδη et al., 2007).

Πλέον, όλα τα Κράτη-Μέλη της ΕΕ, έχουν υιοθετήσει συστήματα διαχείρισης ηλεκτρονικών ταυτοτήτων στο πλαίσιο του εκσυγχρονισμού των ηλεκτρονικά παρεχόμενων υπηρεσιών τους (Λαζαρίδης, 2011). Η εφαρμογή και διαχείριση ηλεκτρονικών ταυτοτήτων συνεχίζει όμως να αποτελεί πρόκληση, δεδομένου ότι περιλαμβάνει εκ των πραγμάτων τη διαχείριση προσωπικών δεδομένων και επομένως ενέχει κινδύνους παραβίασης της ιδιωτικότητας (του προσωπικού απορρήτου) από τη μη εξουσιοδοτημένη πρόσβαση, συλλογή και επεξεργασία προσωπικών ή και ευαίσθητων δεδομένων. Είναι λοιπόν πολύ σημαντικό κάθε λύση ηλεκτρονικής ταυτοποίησης να λαμβάνει πολύ σοβαρά υπόψη θέματα ιδιωτικότητας και να διασφαλίζει την ασφάλεια και προστασία των προσωπικών δεδομένων (Κουντζέρης, 2011). Σύμφωνα και με το Άρθρο 8 του Ευρωπαϊκού Συμφώνου Ανθρωπίνων Δικαιωμάτων (*European Convention on Human Rights*), τα παραπάνω αποτελούν βασικό ανθρώπινο δικαίωμα και η Ευρωπαϊκή Οδηγία 95/46/ΕΚ προβλέπει συγκεκριμένους περιορισμούς για τη διαχείριση προσωπικών δεδομένων. Καθοριστικός παράγοντας, προς αυτή την κατεύθυνση, αποτελεί η σχετική ελευθερία των χωρών να προσδιορίσουν τις ειδικές συνθήκες κάτω από τις οποίες η διαχείριση προσωπικών δεδομένων είναι αποδεκτή και νόμιμη, τις εγγυήσεις που παρέχονται για την προστασία της ιδιωτικότητας, και τις συνθήκες κά-

τω από τις οποίες είναι επιτρεπτή η πρόσβαση σε προσωπικά δεδομένα. Όλα αυτά τα θέματα συνήθως ρυθμίζονται μέσω του νομικού και κανονιστικού πλαισίου (Κουντζέρης, 2010).

4.4 Προσεγγίσεις Ταυτοποίησης

Οι προσεγγίσεις αναφορικά με την ταυτοποίηση οντοτήτων σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης μπορούν να διαχωριστούν σε δύο βασικές κατηγορίες με βάση την αξιοποίηση ενός καθολικού μοναδικού αναγνωριστικού για όλες τις υπηρεσίες, ή εναλλακτικά, διαφορετικών μοναδικών αναγνωριστικών (πολλαπλά αναγνωριστικά ή τομεακά αναγνωριστικά) ανά υπηρεσία ή φορέα παροχής υπηρεσιών (Κουντζέρης, 2010). Είναι προφανές ότι η χρήση ενός καθολικού μοναδικού αναγνωριστικού γενικής χρήσης (*National ID Number*) για όλες τις ηλεκτρονικές υπηρεσίες διευκολύνει τη διαχείριση της ταυτοποίησης και αυθεντικοποίησης στις υπηρεσίες αυτές. Σε αρκετές περιπτώσεις, όμως, τίθενται περιορισμοί από το εκάστοτε εθνικό νομικό και κανονιστικό πλαίσιο, κυρίως σε ζητήματα διασύνδεσης μεταξύ όλων των προσωπικών δεδομένων ενός πολίτη, εγείροντας σημαντικούς περιορισμούς και προβλήματα αναφορικά με την προστασία της ιδιωτικότητάς του (Μήτρου, 2010).

4.5 Αυθεντικοποίηση Ψηφιακών Ταυτοτήτων

Με τον όρο αυθεντικοποίηση νοείται η διαδικασία πιστοποίησης και επιβεβαίωσης της ταυτότητας των χρηστών, η οποία σε κάθε περίπτωση βασίζεται στα διαπιστευτήρια που κατέχει ο χρήστης. Συγκεκριμένα, κατά τη διαδικασία αυθεντικοποίησης αναγνωρίζεται και επιβεβαιώνεται η ορθότητα της ταυτότητας ενός χρήστη ή κάποιων χαρακτηριστικών της. Σε καμία περίπτωση δε θα πρέπει η αυθεντικοποίηση ενός χρήστη να συγχέεται με την παροχή εξουσιοδότησης (*Authorization*) στους πόρους του Π.Σ.

4.5.1 Μηχανισμοί Αυθεντικοποίησης

Τα συστήματα αυθεντικοποίησης είναι δυνατό να κατηγοριοποιηθούν με βάση τη μέθοδο, η οποία αξιοποιείται για την πιστοποίηση της ταυτότητας ενός χρήστη. Οι μέθοδοι αυτοί διαχωρίζονται (Burr et al., 2011) με βάση τα εξής χαρακτηριστικά:

- Κάτι που γνωρίζει (*Something Known*) ο χρήστης, για παράδειγμα ένα συνθηματικό

- Κάτι που κατέχει (*Something Possessed*) ο χρήστης, για παράδειγμα μία έξυπνη κάρτα (*Smart Card*)
- Κάποιο χαρακτηριστικό γνώρισμα (*Something Inherent*), για παράδειγμα βιομετρικές μέθοδοι
- Συνδυασμός κάποιων εκ των ανωτέρω χαρακτηριστικών γνωρισμάτων

Οι μηχανισμοί αυθεντικοποίησης, ανεξάρτητα από τα χαρακτηριστικά που υιοθετούν, αξιοποιούν δύο τύπους κλειδιών:

- Μυστικά κλειδιά: Σε αυτά συμπεριλαμβάνονται τα συνθηματικά, οι κωδικοί και τα συμμετρικά κλειδιά.
- Ασύμμετρα κλειδιά: Σε αυτά συμπεριλαμβάνονται ζεύγη κλειδιών, από τα οποία το ένα είναι δημόσια γνωστό (δημόσιο κλειδί), ενώ το άλλο παραμένει μυστικό (ιδιωτικό κλειδί).

Τα συστήματα αυθεντικοποίησης μπορούν να χαρακτηριστούν ως μονοδιάστατα ή πολυδιάστατα, ανάλογα με τα διαφορετικά χαρακτηριστικά που αξιοποιούν, ώστε να εξασφαλίσουν το επιθυμητό επίπεδο βεβαιότητας για την ταυτότητα κάποιας ηλεκτρονικής οντότητας. Για παράδειγμα, η χρήση ενός ιδιωτικού κλειδιού ως διακριτικού αυθεντικοποίησης, που προστατεύεται από το συνθηματικό του χρήστη, αντιπροσωπεύει ένα χαρακτηριστικό παράδειγμα δισδιάστατου συστήματος αυθεντικοποίησης.

4.6 Διακριτικά Αυθεντικοποίησης

Τα διακριτικά αυθεντικοποίησης αξιοποιούνται για τον έλεγχο της ορθότητας της ψηφιακής ταυτότητας των χρηστών ενός Π.Σ.. Ανάλογα με το επιθυμητό επίπεδο ασφάλειας υιοθετείται και ο αντίστοιχος συνδυασμός χαρακτηριστικών και κλειδιών αυθεντικοποίησης (Ferguson & Schneier, 2003), όπως προαναφέρθηκε στην ενότητα 4.5.

4.6.1 Συνθηματικά

Τα συνθηματικά (*Passwords*) αποτελούν τον ευρύτερα αποδεκτό τρόπο αυθεντικοποίησης, όπου ο χρήστης πιστοποιεί την ορθότητα της ταυτότητάς του, κάνοντας χρήση ενός μυστικού που είναι γνωστό μόνο σε αυτόν. Ο χρήστης πρέπει να απομνημονεύσει το μυστικό κωδικό (*Something known*) και να μην τον αποκαλύπτει σε τρίτες οντότητες.

4.6.2 Διακριτικά Συνθηματικών μιας Χρήσης

Τα διακριτικά συνθηματικών μιας χρήσης (*One-time Password Tokens*) είναι συσκευές υλικού οι οποίες αξιοποιούνται για τη δημιουργία συνθηματικών, τα οποία δεν απαιτείται να απομνημονεύει ο χρήστης και τα οποία χρησιμοποιούνται μόνο μια φορά. Η παραγωγή των συνθηματικών στηρίζεται σε συγκεκριμένους αλγόριθμους κρυπτογράφησης. Η επαναχρησιμοποίηση ενός κωδικού για μελλοντική αυθεντικοποίηση του χρήστη δεν είναι δυνατή.

4.6.3 Διακριτικά Χαλαρής Αποθήκευσης

Τα διακριτικά χαλαρής αποθήκευσης (*Soft Tokens*) αναφέρονται σε μυστικά κλειδιά, τα οποία αποθηκεύονται σε κάποιο μέσο αποθήκευσης όπως σκληρός δίσκος, CD, USB token κ.λπ. Τα κλειδιά είναι αποθηκευμένα σε κρυπτογραφημένη μορφή, ενώ η προσπέλασή τους είναι δυνατή μόνο με τη χρήση του κατάλληλου συνθηματικού.

4.6.4 Διακριτικά Υλικού – Σκληρής Αποθήκευσης

Τα διακριτικά υλικού σκληρής αποθήκευσης (*Hard Tokens*) αναφέρονται σε συσκευές υλικού, οι οποίες αποθηκεύουν τα απαιτούμενα μυστικά κλειδιά και προσφέρουν απαραβίαστη (*Tamper Proof*) προστασία. Όλες οι κρυπτογραφικές διαδικασίες πραγματοποιούνται εσωτερικά στη συσκευή και συνεπώς δεν υπάρχει καμία δυνατότητα ανάγνωσης των κλειδιών από εξωτερικές οντότητες. Για την ενεργοποίηση των κλειδιών συνηθίζεται η χρήση κάποιου συνθηματικού.

4.7 Ψηφιακά Πιστοποιητικά X.509 v3

Το πρότυπο X.509 για ψηφιακά πιστοποιητικά προτάθηκε το 1988 από τη Διεθνή Ένωση Τηλεπικοινωνιών (*International Telecommunications Union – ITU*) και έκτοτε αποτελεί πρότυπο για την πιστοποίηση χρηστών. Διαθέτει αρκετά προκαθορισμένα πεδία για την αναγραφή των απαραίτητων πληροφοριών. Η τρίτη έκδοσή του, X.509 v3, παρέχει τη δυνατότητα, εκτός από τις προκαθορισμένες πληροφορίες, να συμπεριλαμβάνονται και επιπλέον εκτεταμένα πεδία (extensions) ανάλογα την εφαρμογή τους, τα οποία καθορίζονται από τον Εκδότη των πιστοποιητικών (issuer). Στον Πίνακας 4-1 που ακολουθεί, παρουσιάζεται η γενική δομή ενός ψηφιακού πιστοποιητικού τύπου X.509 v3.

Πεδίο	Field
Έκδοση	Version
Αριθμός Σειράς	Serial Number
Αλγόριθμος Υπογραφής	Signature Algorithm
Διακριτικό Όνομα Εκδότη	Issuer DN
Ισχύει Από	Valid From
Ισχύει Μέχρι	Valid To
Διακριτικό Όνομα Υποκειμένου	Subject DN
Δημόσιο Κλειδί Υποκειμένου	Subject Public Key
Μοναδικό Αναγνωριστικό Εκδότη	Issuer Unique Identifier
Μοναδικό Αναγνωριστικό Υποκειμένου	Subject Unique Identifier
Επεκτάσεις	Extensions
Ψηφιακή Υπογραφή	Certification Authority's Digital Signature

Πίνακας 4-1: Βασικά Πεδία Ψηφιακού Πιστοποιητικού X.509 v3

Αναλυτικότερα, τα πεδία αυτά είναι:

- *Έκδοση (Version)*: αναφέρεται στην έκδοση του προτύπου X.509 πιστοποιητικών και υποστηρίζει εκτεταμένα πεδία.
- *Αριθμός Σειράς (Serial Number):* αποτελείται από το μοναδικό αριθμό του εκδιδόμενου πιστοποιητικού, ο οποίος καθορίζεται από τον εκδότη των πιστοποιητικών με σκοπό τη διάκριση του πιστοποιητικού.
- *Αλγόριθμός Υπογραφής (Signature Algorithm):* αναφέρεται στον αλγόριθμό σύνοψης (Hash Function) που θα αξιοποιείται από την ΥΔΚ. Προτείνεται η αξιοποίηση του SHA-1.
- *Διακριτικό Όνομα Εκδότη (Issuer DN):* αναφέρεται στο όνομα του εκδότη του πιστοποιητικού και αποτελείται από τα υπό-πεδία Χώρα (*Country*), Οργανισμός (*Organization*), Κοινό Όνομα (*Common Name*) και Ηλεκτρονική Διεύθυνση (*E-mail Address*). Όλα τα παραπάνω πεδία, πλην αυτού της Ηλεκτρονικής Διεύθυνσης, είναι υποχρεωτικά.
- *Ισχύει Από (Valid From):* περιλαμβάνει την ημερομηνία έκδοσης του πιστοποιητικού.

- *Ισχύει Μέχρι (Valid To):* περιλαμβάνει την ημερομηνία λήξης του πιστοποιητικού.
- *Διακριτικό Όνομα Υποκειμένου (Subject DN):* Αναφέρεται στον κάτοχο του πιστοποιητικού και αποτελείται από τα υπό-πεδία Χώρα (*Country*), Οργανισμός (*Organization*), Κοινό Όνομα (*Common Name*) και Ηλεκτρονική Διεύθυνση (*E-mail Address*). Τα παραπάνω πεδία, πλην της αυτό της Ηλεκτρονικής Διεύθυνσης, είναι υποχρεωτικά. Σύμφωνα με το RFC 3280, η χρήση της ηλεκτρονικής διεύθυνσης στο συγκεκριμένο πεδίο προτείνεται μόνο σε περιπτώσεις που απαιτείται συμβατότητα με προϋπάρχουσες υπηρεσίες και εφαρμογές.
- *Δημόσιο Κλειδί Υποκειμένου (Subject Public Key):* αποτελείται από το Δημόσιο Κλειδί του Υποκειμένου (Ιδιοκτήτη του ψηφιακού πιστοποιητικού).
- *Επεκτάσεις (Extensions)*
    - *Χρήση Κλειδιού (Key Usage)*: αναφέρεται ποια θα είναι η χρήση του δημόσιου κλειδιού που περιλαμβάνεται στο ψηφιακό πιστοποιητικό. Καθώς το τομεακό πιστοποιητικό χρησιμεύει μόνο για επαλήθευση Ψηφιακής Υπογραφής, τα πεδία που ορίζονται είναι τα "digitalSignature" και "nonRepudiation".
    - *Εναλλακτικό Όνομα Υποκειμένου (Subject Alternative Name)*: περιλαμβάνεται ένα εναλλακτικό όνομα για τον κάτοχο του ψηφιακού πιστοποιητικού. Δεδομένης της ταυτόχρονης ύπαρξης του πεδίου *Διακριτικό Όνομα Υποκειμένου (Subject DN)*, στο παρόν πεδίο θα περιληφθεί κρυπτογραφημένο (αξιοποιώντας τις οδηγίες του κάποιου προτύπου όπως το PKCS#1) το σχετικό αναγνωριστικό του χρήστη που επιθυμεί ο δημόσιος φορέας που προσφέρει την υπηρεσία (π.χ. ΑΦΜ).
    - *Ταυτοποίηση Χρήστη (Clientauth)*: αναφέρει, εάν το συγκεκριμένο πιστοποιητικό μπορεί να χρησιμοποιηθεί για την ταυτοποίηση του χρήστη. Στα τομεακά ψηφιακά πιστοποιητικά, το συγκεκριμένο πεδίο ορίζεται (set).
    - Σημεία Διανομής Καταλόγου Ανακληθέντων Πιστοποιητικών (*CRL Distribution List*): αναφέρονται τα σημεία διανομής της Λίστας Ανακληθέντων Πιστοποιητικών, σε μορφή URL διεύθυνσης.

- Ψηφιακή Υπογραφή (*Certification Authority's Digital Signature*): αποτελείται από την ψηφιακή υπογραφή του εκδότη του ψηφιακού πιστοποιητικού.

4.7.1 Αποθήκευση Μοναδικού Αναγνωριστικού

Το RFC 4683 με τίτλο "*Internet X.509 Public Key Infrastructure Subject Identification Method (SIM)*" προτάθηκε το 2006 από το Internet Engineering Task Force (IETF) και προτείνει την ενσωμάτωση ευαίσθητων προσωπικών αναγνωριστικών στο πεδίο *otherName* της επέκτασης *subjectAltName* των ψηφιακών πιστοποιητικών των τελικών χρηστών τύπου X.509 (Park et al., 2006). Ο τελικός χρήστης αναγνωρίζεται από ευαίσθητες πληροφορίες αναγνώρισης (Sensitive Identification Information (SII)), που σχετίζονται με συγκεκριμένο τύπο (*Sensitive Identification Information type (SIItype)*). Ο χρήστης επιλέγει ένα συνθηματικό (*P*) και, μαζί με το SIItype και SII τα προωθεί στην Αρχή Εγγραφής (*Registration Authority (RA)*), κάνοντας χρήση ενός ασφαλούς δίαυλου επικοινωνίας (*Secure Communication Channel*). Η Αρχή Εγγραφής επιβεβαιώνει την εγκυρότητα των στοιχείων, παράγει μία τυχαία τιμή *R* και υπολογίζει την τιμή της *SIM* σύμφωνα με τις παραστάσεις (1) και (2), όπου *H()* είναι μία κρυπτογραφικά ασφαλής μονόδρομη συνάρτηση σύνοψης (*Hash Function*). Η τιμή της *SIM* αποστέλλεται στο χρήστη και στην Αρχή Πιστοποίησης (*Certification Authority (CA)*), η οποία εκδίδει το ψηφιακό Πιστοποιητικό X.509, συμπεριλαμβάνοντάς την στο πεδίο *otherName* της επέκτασης *subjectAltName*, κάθε φορά που ο χρήστης αιτείται την έκδοση ψηφιακού πιστοποιητικού (*Digital Certificate*).

$$PEPSI = H\,(\,H\;\,(\,P \,||\, R \,||\, SIItype \,||\, SII\,)\,)\,. \qquad (\mathbf{1})$$

$$SIM = R \,||\, PEPSI\,. \qquad (\mathbf{2})$$

$$PEPSI' = H\,(\,H\;\,(\,P \,||\, R \,||\, SIItype \,||\, SII\,)\,)\,. \qquad (\mathbf{3})$$

$$SIM' = R \,||\, PEPSI'\,. \qquad (\mathbf{4})$$

$$H\;\,(\,P \,||\, R \,||\, SIItype \,||\, SII\,)\,. \qquad (\mathbf{5})$$

Κάθε φορά που ο χρήστης αιτείται την παροχή μιας ηλεκτρονικής υπηρεσίας σε κάποιον πάροχο (*Service Provider*), θα πρέπει να του αποστείλει, μέσω ασφαλούς καναλιού επικοινωνίας, τα *SII*, *SIItype*, *P*, καθώς και το ψηφιακό πιστοποιητικό του. Μετά την επιτυχή παραλαβή τους, ο πάροχος υπολογίζει τις τιμές των *PEPSI'* και *SIM'* σύμφωνα με τις παραστάσεις (3) και

(4), συγκρίνει την τιμή της *SIM'* με την τιμή *SIM* που υπάρχει στο ψηφιακό πιστοποιητικό του χρήστη και επαληθεύει την ορθότητα του *PII* που υπέβαλε ο χρήστης. Σε περιπτώσεις όπου ο πάροχος γνωρίζει εκ των προτέρων το SII του χρήστη και μένει να αποδειχθεί ότι είναι όντως ο κάτοχός τους, ο χρήστης αποστέλλει στον πάροχο το ψηφιακό πιστοποιητικό και το συνθηματικό *P*. Τέλος, σε περίπτωση που ο χρήστης θέλει να αποδείξει στον πάροχο ότι είναι κάτοχος ενός *SII*, χωρίς όμως να το αποστείλει, μπορεί να υποβάλει το αποτέλεσμα της παράστασης (5), που αποτελεί ενδιάμεση τιμή της (1) μαζί με το ψηφιακό πιστοποιητικό του. Ο πάροχος μπορεί να υπολογίσει το *R* από την τιμή του *SIM*, που είναι αποθηκευμένο στο ψηφιακό πιστοποιητικό του χρήστη, να υπολογίσει την τιμή της συνάρτησης (5) και να επιβεβαιώσει ότι ο χρήστης όντως γνωρίζει το *P* και το *SII*.

Η συγκεκριμένη μέθοδος αποθήκευσης ψηφιακών αναγνωριστικών θα μπορούσε να εφαρμοστεί από κράτη που αξιοποιούν ενιαία μοναδικά αναγνωριστικά (Hayat et al., 2004), ειδικότερα για την παροχή ηλεκτρονικών υπηρεσιών, καθώς ο χρήστης μπορεί να αναγνωριστεί μοναδικά από τον πάροχο, ασχέτως της ζητούμενης υπηρεσίας. Επιπρόσθετα, μπορεί να διευκολύνει και να προωθήσει τη διαλειτουργικότητα και την ανταλλαγή δεδομένων και πληροφοριών μεταξύ των παρόχων για κάθε χρήστη.

4.7.2 Αποθήκευση Πολλαπλών Αναγνωριστικών

Δεδομένου ότι δεν είναι εφικτή η αξιοποίηση των μοναδικών αναγνωριστικών σε όλα τα Π.Σ. Ηλεκτρονικής Διακυβέρνησης, προτείνεται μία μέθοδος αποθήκευσης πολλαπλών αναγνωριστικών σε ψηφιακά πιστοποιητικά X.509 v3, αξιοποιώντας την υπάρχουσα υποδομή Δημοσίου Κλειδιού (*PKI*). Η εφαρμογή της μπορεί να προωθήσει τη διαλειτουργικότητα σε περιβάλλοντα όπου δεν είναι εφικτή η αξιοποίηση μοναδικών αναγνωριστικών, αλλά και να καταστήσει δυνατή την ταυτοποίηση των χρηστών μεταξύ διαφορετικών περιβαλλόντων και Π.Σ. Η διαφοροποίησή, σε σχέση με το RFC 4683, έγκειται στην ύπαρξη πολλαπλών συνθηματικών (P), PEPSI και τιμών SIM, μία για κάθε αναγνωριστικό χρήστη, καθώς και ενός καθολικό συνθηματικό P_{master}.

Έστω ότι στον χρήστη Α έχουν ανατεθεί *n* αναγνωριστικά (ID_1, ID_2 … ID_n) και το καθένα από αυτά αντιστοιχεί σε κάποιο συγκεκριμένο SIItype. Καθένα από αυτά θα πρέπει να συσχετίζεται με ένα μοναδικό συνθηματικό P_{IDx}, όπου $x=\{1,2,3,\ldots,n-1,n\}$. Καθώς, όμως, η επιλογή και απομνημόνευση από το χρήστη, *n* διαφορετικών ισχυρών συνθηματικών δεν είναι πρακτική από πλευράς διαχείρισης συνθηματικών, ο χρήστης επιλέγει ένα καθολικό συνθηματικό P_{master}, το

οποίο αξιοποιείται για τη δημιουργία των απαιτούμενων *n* μοναδικών συνθηματικών P_{IDx}, με βάση την παράσταση (6), όπου το *H( )* είναι ένας ασφαλής κρυπτογραφικός αλγόριθμος σύνοψης (*Hash Function*). Η συνένωση των P_{master} και SIItype διασφαλίζει ότι κάθε συνθηματικό θα είναι μοναδικό, σε σχέση με τα υπόλοιπα, καθώς δύο αναγνωριστικά δεν μπορούν να αντιστοιχούν στο ίδιο SIItype, ενώ η αξιοποίηση ασφαλούς κρυπτογραφικού αλγόριθμου σύνοψης διασφαλίζει ότι το καθολικό συνθηματικό , και κατά συνέπεια κάθε συνθηματικό P_{IDx}, δεν μπορεί να αποκαλυφθεί σε μη εξουσιοδοτημένες οντότητες.

$$P_{IDx} = H\,(P_{master} \,||\, SIItype\,) \qquad x=\{1,2,3,\ldots,n\text{-}1,n\} \tag{6}$$

$$PEPSI_{IDx} = H\,(\,H\;\,(P_{IDx} \,||\, R_{IDx} \,||\, SIItype \,||\, IDx\,)\,) \qquad x=\{1,2,3,\ldots,n\text{-}1,n\} \tag{7}$$

$$SIM_{IDx} : (\,R_{IDx} \,||\, PEPSI_{IDx}) \qquad x=\{1,2,3,\ldots,n\text{-}1,n\} \tag{8}$$

$$SIM_{total} : (\,SIM_{IDx} \,||\, SIM_{IDx\,+1} \,||\, SIM_{IDx\,+2} \,||\, \ldots \,||\, SIM_{IDn-1} \,||\, SIM_{IDn}\,) \qquad x=\{1,2,3,\ldots,n\text{-}1,n\} \tag{9}$$

Αρχικά, ο χρήστης επιλέγει ένα ισχυρό καθολικό συνθηματικό P_{master}, υπολογίζει το P_{IDx} συνθηματικό για κάθε αναγνωριστικό και ενημερώνει την Αρχή Εγγραφής, μέσω ασφαλούς διαύλου επικοινωνίας, για τα αναγνωριστικά, τον SIItype τύπο τους και τα αντίστοιχα συνθηματικά. Ο χρήστης έχει τη δυνατότητα να υποβάλει λιγότερα αναγνωριστικά από αυτά που έχουν συσχετιστεί με την ψηφιακή του ταυτότητα, αλλά για λόγους απλότητας θεωρείται ότι τα υποβάλλει όλα εξ' αρχής. Στην περίπτωση όπου γινόταν αυτό, το αντίστοιχο πεδίο στην παράσταση (9) θα συμπεριλαμβανόταν ως κενό. Η Αρχή Εγγραφής, με τη σειρά της, επαληθεύει τη συσχέτιση των συγκεκριμένων αναγνωριστικών τόσο με την ψηφιακή ταυτότητα του χρήστη όσο και το SII type και παράγει μία τυχαία τιμή R_{IDx} για κάθε αναγνωριστικό. Η παραγωγή της συγκεκριμένης τιμής πρέπει να πραγματοποιείται από μία γεννήτρια τυχαίων αριθμών (*Random Number Generator (RNG)*) που πληροί κατ' ελάχιστον τις απαιτήσεις που ορίζονται στο FIPS 140-2 (NIST, 2002) και το μήκος της είναι υποχρεωτικά όμοιο με την έξοδο του αλγόριθμου σύνοψης που αξιοποιείται από την Αρχή Εγγραφής. Έχοντας παράξει *n* τυχαίες τιμές (R_{ID1}, R_{ID2}, ... P_{IDn}), η Αρχή Εγγραφής υπολογίζει αντίστοιχα *n* PEPSI τιμές, μία για κάθε αναγνωριστικό, με βάση την παράσταση (7),

όπου πάλι το *H( )* είναι ένας ασφαλής κρυπτογραφικός αλγόριθμος σύνοψης. Στη συνέχεια υπολογίζει την SIM_{IDx}, πάλι για κάθε αναγνωριστικό, με βάση την παράσταση (8). Παρόμοια με το RFC 4683, που περιγράφηκε στην ενότητα 4.7.1, η τιμή SIM_{ID} αποτελείται από τη συνένωση του $PEPSI_{ID}$ και μιας τυχαίας τιμής. Τέλος, υπολογίζει την τιμή της SIM_{total} συνενώνοντας όλα τα SIM_{IDx} σύμφωνα με την παράσταση (9).

Δεδομένου ότι το συνολικός αριθμός των αναγνωριστικών που μπορούν να αξιοποιηθούν σε ένα περιβάλλον, είναι προκαθορισμένος, αντίστοιχα μπορεί να προκύψει συγκεκριμένος αριθμός τιμών SIM_{ID}. Ως εκ τούτου, μια προκαθορισμένη ακολουθία τμημάτων ίδιου μεγέθους επιτρέπει την εύκολη αναζήτηση και ανεύρεση κάθε τιμής SIM_{ID} και κατά συνέπεια κάθε $PEPSI_{ID}$ και R_{ID}. Όπως αναφέρθηκε και προηγουμένως, σε περιπτώσεις όπου ο χρήστης δεν επιθυμεί να υποβάλει κάποιο συγκεκριμένο αναγνωριστικό, το αντίστοιχο SIM_{ID} δεν μπορεί να αντικαθίσταται από άλλο προκειμένου για διασφαλιστεί η ακολουθία τους. Τέλος, η Αρχή Εγγραφής ενημερώνει το χρήστη Α για την τιμή της SIM_{total} και την αποστέλλει, μέσω ασφαλούς καναλιού επικοινωνίας στην Αρχή Πιστοποίησης Πλέον σε κάθε έκδοση ψηφιακού πιστοποιητικού για το συγκεκριμένο χρήστη, η Αρχή Πιστοποίησης συμπεριλαμβάνει τη συγκεκριμένη τιμή στο πεδίο *otherName* της επέκτασης *subjectAltName*.

Κάθε φορά που ο χρήστης αιτείται την παροχή συγκεκριμένης ηλεκτρονικής υπηρεσίας, θα πρέπει να αποστείλει στον πάροχο το κατάλληλο αναγνωριστικό, καθώς και να αποδείξει ότι όντως το συγκεκριμένο αναγνωριστικό τον προσδιορίζει μοναδικά. Υπάρχουν όμως και περιπτώσεις κατά τις οποίες ο πάροχος έχει προηγούμενη γνώση (*Prior Knowledge*) για το αναγνωριστικό του χρήστη ή περιπτώσεις, όπου απαιτείται μόνο η πληροφορία ότι έχει όντως πραγματοποιηθεί ανάθεση στο χρήστη συγκεκριμένου τύπου αναγνωριστικού. Η συγκεκριμένη πρόταση μπορεί να ικανοποιήσει όλες τις παραπάνω περιπτώσεις, με βάση τα δεδομένα που υποβάλλει ο χρήστης.

Στην πρώτη περίπτωση, που είναι και η πιο συνηθισμένη, ο πάροχος της υπηρεσίας δεν έχει καμία εκ των προτέρων πληροφορία για την ψηφιακή ταυτότητα του χρήστη Α. Ως εκ τούτου ο χρήστης αιτείται την παροχή συγκεκριμένης υπηρεσίας και αποστέλλει μέσω ασφαλούς καναλιού επικοινωνίας το αναγνωριστικό, το αντίστοιχο SIItype, το συνθηματικό για το συγκεκριμένο αναγνωριστικό (P_{ID}), καθώς και το Ψηφιακό Πιστοποιητικό του. Ο πάροχος μπορεί πλέον να υπολογίσει την τιμή της $PEPSI'_{ID}$ με βάση την παράσταση (10) και, γνωρίζοντας τη σειρά με την οποία αποθηκεύεται κάθε SIM_{ID} στο SIM_{total}, να το συγκρίνει με το SIM'_{ID}. Σε περίπτωση που υπάρχει ταύτιση των δύο τιμών, επιβεβαιώνεται η ορθότητα των πληροφοριών που απέστειλε ο χρήστης Α και μπορεί πλέον να του παρασχεθεί η ηλεκτρονική υπηρεσία που αιτήθηκε.

$$PEPSI'_{ID} = H\,(\,H\;\;(P_{ID} \,||\, R_{ID} \,||\, SIItype \,||\, ID\,)\,) \qquad (\mathbf{10})$$

$$SIM'_{ID} : (\,R_{ID} \,||\, PEPSI'_{ID}) \qquad (\mathbf{11})$$

$$H\;\;(P_{ID} \,||\, R_{ID} \,||\, SIItype \,||\, ID\,) \qquad (\mathbf{12})$$

Στη δεύτερη περίπτωση. όπου ο πάροχος γνωρίζει το αναγνωριστικό του χρήστη και απαιτείται μόνο η απόδειξη ότι όντως τον προσδιορίζει μοναδικά, ο χρήστης αποστέλλει το συνθηματικό για το συγκεκριμένο αναγνωριστικό (P_{ID}) καθώς και το Ψηφιακό Πιστοποιητικό του. Ο πάροχος υπολογίζει την τιμή της $PEPSI'_{ID}$ με βάση την παράσταση (10) και γνωρίζοντας τη σειρά με την οποία αποθηκεύεται κάθε SIM_{ID} στο SIM_{total}, να το συγκρίνει με το SIM'_{ID}. Στην τρίτη περίπτωση όπου ο χρήστης δεν επιθυμεί να αποστείλει το αναγνωριστικό του στον πάροχο της υπηρεσίας, αλλά μόνο να αποδείξει ότι όντως του έχει ανατεθεί αναγνωριστικό συγκεκριμένου SIItype, υπολογίζει την τιμή της παράστασης (12) και την αποστέλλει στον πάροχο μαζί με το Ψηφιακό Πιστοποιητικό του. Για τον υπολογισμό της συγκεκριμένης τιμής, ο χρήστης αξιοποιεί το R_{ID} από το αντίστοιχο SIM_{ID}, που είναι αποθηκευμένο στο Ψηφιακό Πιστοποιητικό του. Αντίστοιχα, ο πάροχος αξιοποιεί το ίδιο R_{ID}, υπολογίζει τη σύνοψη της παράστασης που απέστειλε ο χρήστης, την ενώνει με το R_{ID} και ελέγχει, εάν το αποτέλεσμα είναι ίδιο με το SIM_{ID} που βρίσκεται αποθηκευμένο στο ψηφιακό πιστοποιητικό του χρήστη.

Σε μία Υποδομή Δημόσιου Κλειδιού, τα Ψηφιακά Πιστοποιητικά των χρηστών είναι δημόσια διαθέσιμα, και ως εκ τούτου θα πρέπει να διασφαλιστεί η ιδιωτικότητα των αναγνωριστικών που περιλαμβάνονται σε αυτά, με βάση τη συγκεκριμένη πρόταση. Προκειμένου να ικανοποιηθεί η συγκεκριμένη απαίτηση γίνεται επαναλαμβανόμενη χρήση ασφαλών κρυπτογραφικών συναρτήσεων στο κάθε αναγνωριστικό (ID), στο συνθηματικό του κάθε αναγνωριστικού (P_{ID}) και στην κάθε τυχαία τιμή (R_{ID}). Δεδομένου ότι έχουν εντοπιστεί αρκετά κενά ασφάλειας στον αλγόριθμο SHA-1 (Schneier, 2005) προτείνεται η αξιοποίηση του SHA-2 ή κάποιου πιο ασφαλούς αλγόριθμου. Για την επιλογή του καθολικού συνθηματικού P_{master}, ο χρήστης θα πρέπει να επιλέγει συνθηματικά που θα ικανοποιούν κατ' ελάχιστον τις απαιτήσεις που αναφέρονται στα πρότυπα FIPS 112 και FIPS 180-4 (NIST, 1985) (NIST, 2012), και οι τυχαίες τιμές (R_{ID}) θα πρέπει να παράγονται από μία γεννήτρια τυχαίων αριθμών που ικανοποιεί κατ ελάχιστον τις απαιτήσεις που αναφέρονται στο πρότυπο FIPS 140-2 (NIST, 2002).

4.8 Ομόσπονδες Ταυτότητες

Ως Ομοσπονδία (*Federation*) ορίζεται "*το σύνολο δύο ή περισσοτέρων επιχειρηματικών συνεργατών που έχουν κοινούς χρήστες και στοχεύουν στην αναβάθμιση της ποιότητας των προσφερόμενων υπηρεσιών ταυτόχρονα με τη μείωση του κόστους διαχείρισης των ψηφιακών ταυτοτήτων τους*" (Buecker et al., 2008). Ως αποτέλεσμα δημιουργίας της ομοσπονδίας, οι συμμετέχοντες μπορούν να αναπτύξουν και να αξιοποιήσουν εφαρμογές βασισμένες στην ψηφιακή ταυτότητα των χρηστών τους (*Identity-Based Applications*), διευκολύνοντας και απλοποιώντας την πρόσβαση σε υπηρεσίες και πληροφορίες χωρίς την ανάγκη για δημιουργία ή εκ νέου αντιστοίχηση των ψηφιακών ταυτοτήτων μέσα στην ομοσπονδία (Baldoni, 2012). Η εγκαθίδρυση μίας ομοσπονδίας βασίζεται στην εγκαθίδρυση αμοιβαίων σχέσεων εμπιστοσύνης. Οι σχέσεις αυτές δημιουργούνται χρησιμοποιώντας νομικές συμφωνίες (*Agreements*) μεταξύ των συμμετεχόντων, και είναι απαραίτητο να ισχύσουν πριν την έναρξη λειτουργίας της. Τέτοιες συμφωνίες συνήθως περιλαμβάνουν και τις τεχνολογίες – μεθοδολογίες, που θα υποστηρίζουν την ομοσπονδία, και περιλαμβάνουν κατ' ελάχιστον τις δυνατότητες διαχείρισης της ομοσπονδίας και της μεταξύ τους εμπιστοσύνης, την κρυπτογραφική υποστήριξη, καθώς και τα πρωτόκολλα και τις επιχειρηματικές διαδικασίες βάσει των οποίων πραγματοποιείται μία συναλλαγή.

Στην τεχνολογία πληροφορίας (*IT*), η ομόσπονδη ταυτότητα (*Federated Identity*) έχει δύο βασικές έννοιες (Buecker et al., 2008):

- Τη διαδικασία αυθεντικοποίησης ενός χρήστη, διαμέσου διαφορετικών Π.Σ. ή οργανισμών.
- Την εικονική ένωση (*Assembled Identity*) των πληροφοριών ενός χρήστη (ή μιας αρχής), που είναι αποθηκευμένες σε πολλαπλά διακριτά συστήματα διαχείρισης ταυτότητας. Τα δεδομένα συνενώνονται μεταξύ τους χρησιμοποιώντας ένα κοινό στοιχείο, συνήθως το όνομα του χρήστη.

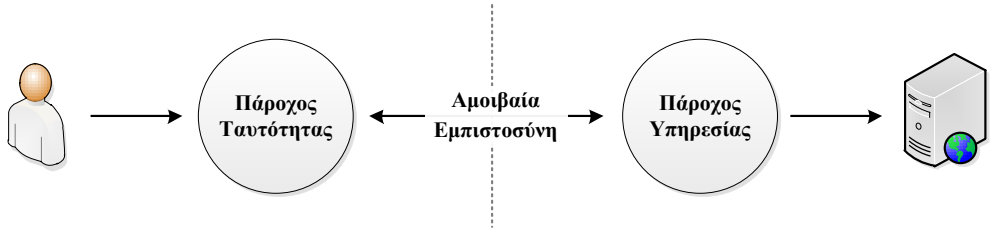
4.8.1 Διαχείριση Ομόσπονδης Ταυτότητας

Μία βασική απαίτηση για την εγκαθίδρυση και ομαλή λειτουργία μίας ομοσπονδίας είναι η αποτελεσματική και συνεπής διαχείριση των ψηφιακών ταυτοτήτων. Η συγκεκριμένη διαδικασία αυτή ονομάζεται "*Διαχείριση Ομόσπονδης Ταυτότητας*" (*Federated Identity Management*) (Pfitzmann & Waidner, 2003) και εστιάζει στον προσδιορισμό (Baldwin et al., 2008):

- των διαδικασιών και υπηρεσιών που απαιτούν ταυτοποίηση των χρηστών,

- του βαθμού βεβαιότητας για την πραγματική ταυτότητα του χρήστη,
- της διακριτικής προσπέλασης των χρηστών από τις παρεχόμενες υπηρεσίες και
- των εργαλείων που θα διαχειρίζονται τις ψηφιακές ταυτότητες των χρηστών.

Σύμφωνα με τους (Jøsang & Pope, 2005), η διαχείριση ομόσπονδων ταυτοτήτων ορίζεται ως "*ένα σύνολο συμφωνιών, προτύπων και τεχνολογιών που επιτρέπουν σε μια ομάδα παρόχων ηλεκτρονικών υπηρεσιών να αναγνωρίσουν τα αναγνωριστικά χρήστη και δικαιώματα από άλλους παρόχους υπηρεσιών που συμμετέχουν στην ομοσπονδία*". Οι σημαντικότεροι ρόλοι (*Roles*) σε μια ομοσπονδία είναι ο πάροχος ταυτότητας (*Identity Provider*) και ο πάροχος υπηρεσίας (*Service Provider*) (Buecker et al., 2008). Ο πάροχος ταυτότητας είναι υπεύθυνος για τη διαχείριση των χρηστών και των ταυτοτήτων τους, για την έκδοση πιστοποιητικών, την αυθεντικοποίησή τους, και εγγυάται για την ταυτότητα των χρηστών. Ο πάροχος υπηρεσιών είναι υπεύθυνος για τον έλεγχο πρόσβασης σε υπηρεσίες, επικυρώνει τις πληροφορίες των ταυτοτήτων για τον πάροχο ταυτότητας, παρέχει πρόσβαση βασιζόμενος στις ταυτότητες και διαχειρίζεται μόνο τοπικά χαρακτηριστικά των χρηστών και όχι ολόκληρο το προφίλ τους. Η αμοιβαία εμπιστοσύνη μεταξύ των δύο παρόχων που δημιουργείται σε μία ομοσπονδία παρουσιάζεται στο Σχήμα 4-4 στη συνέχεια.



Σχήμα 4-4: Ομοσπονδία με Πάροχο Ταυτότητας και Πάροχο Υπηρεσιών (Buecker et al., 2008)

Σε κάποια επιχειρησιακά σενάρια ένας οργανισμός μπορεί να ενεργεί τόσο ως πάροχος ταυτότητας όσο και ως πάροχος υπηρεσιών. Για παράδειγμα, όταν κάποιες δημόσιες υπηρεσίες έχουν πρόσβαση στις μεταξύ τους εφαρμογές, κάθε υπηρεσία παίζει το ρόλο είτε του παρόχου ταυτότητας είτε των παρόχου υπηρεσιών, βασιζόμενη στο ποιος οργανισμός παρέχει τις εφαρμογές σε κάθε περίπτωση. Το σκεπτικό που οδήγησε στη δημιουργία ομόσπονδων ταυτοτήτων, είναι ότι η υπάρχουσα, ετερογενής φύση των αρχιτεκτονικών των πληροφοριακών συστημάτων των οργανισμών δεν θα πρέπει να είναι αναγκαίο να αλλάξει. Ο στόχος των ομόσπονδων ταυτοτήτων είναι να επιτυγχάνεται, αποδοτικά και με ασφάλεια, η πρόσβαση σε πόρους διαφορετικών οργα-

νισμών, με αποτέλεσμα να αυξάνεται η παραγωγικότητα, η λειτουργική αποδοτικότητα και η ανταγωνιστική διαφοροποίηση.

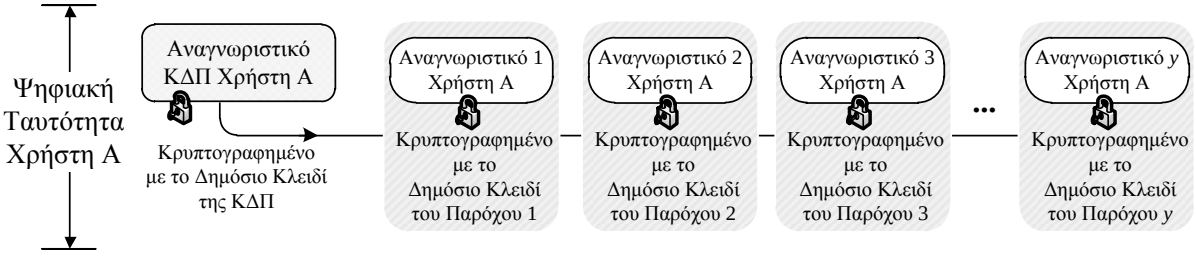
4.8.2 Αξιοποίηση Ομόσπονδων Ταυτοτήτων σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης

Όπως αναφέρθηκε και την ενότητα 2.2, η διαλειτουργικότητα αποτελεί βασική απαίτηση και προτεραιότητα των σύγχρονων Π.Σ. Ηλεκτρονικής Διακυβέρνησης, επιτρέποντας τη μεταφορά και αξιοποίηση δεδομένων από τα επιμέρους Π.Σ. των Δημόσιων Φορέων. Ο σχεδιασμός και υλοποίηση μιας ομόσπονδης αρχιτεκτονικής *(Federated Architecture*) μπορεί να καταστήσει δυνατή την αλληλεπίδραση μεταξύ τους, επιτρέποντάς τους να διατηρήσουν την αυτονομία τους. Οι υφιστάμενες τεχνολογικές λύσεις για την υλοποίηση αρχιτεκτονικών ομόσπονδης διαχείρισης ταυτοτήτων ορίζουν ένα σύνολο πρωτοκόλλων για την ασφαλή ανταλλαγή πληροφορικών σχετικών με την ψηφιακή ταυτότητα των οντοτήτων που συμμετέχουν στην ομοσπονδία. Επίσης, υιοθετούν προσεγγίσεις βασισμένες στην τεχνολογία Security Assertion Markup Language (*SAML*). Πρότυπα και προδιαγραφές όπως Liberty ID-FF (Liberty Alliance, 2006), Liberty ID-WSF (Liberty Alliance, 2006), Liberty IGF Privacy Constraints (Liberty Alliance, 2007), WS-Policy (OASIS, 2006) και WS-Trust (OASIS, 2007) παρέχουν χρήσιμες οδηγίες για τον τρόπο υλοποίησης των μηχανισμών επικοινωνίας και ανταλλαγής δεδομένων.

4.8.3 Χρήση Πολλαπλών Αναγνωριστικών

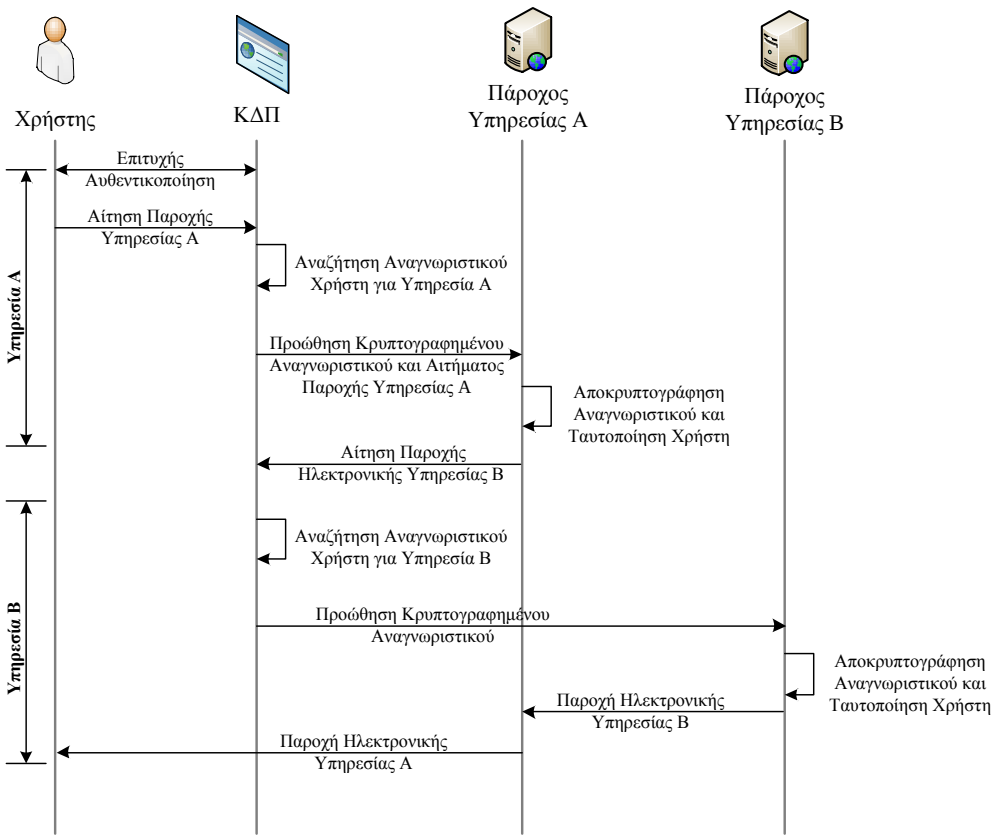
Στις περιπτώσεις, όπου η Δημόσια Διοίκηση αξιοποιεί πολλαπλά αναγνωριστικά, το πρόβλημα που δημιουργείται, είναι η ταυτοποίηση των χρηστών, καθώς απαιτούνται πολλαπλοί πάροχοι ταυτότητας. Για την επίλυση του συγκεκριμένου προβλήματος, προτείνεται η αξιοποίηση της υπάρχουσας υποδομής Δημοσίου Κλειδιού και η δημιουργία μίας αλληλουχίας αναγνωριστικών, που θα αποθηκεύεται στην Κεντρική Διαδικτυακή Πύλη, σε συνδυασμό με ένα καινούργιο αναγνωριστικό που θα ανατίθεται από αυτή σε κάθε αλληλουχία, και κατά συνέπεια στον κάθε χρήστη. Η συγκεκριμένη αλληλουχία αναγνωριστικών, που παρουσιάζεται στο Σχήμα 4-5 παρακάτω, θα έχει προκαθορισμένο μέγεθος, που θα καθορίζεται από το σύνολο των παρόχων που προσφέρουν τις υπηρεσίες τους ηλεκτρονικά. Σε κάθε πάροχο θα αντιστοιχίζεται υποχρεωτικά ένα συγκεκριμένο κομμάτι (*Block*) της αλληλουχίας και ενδεχόμενη προσθήκη καινούργιου παρόχου, άρα και τμήματος στην αλληλουχία, θα πρέπει να πραγματοποιείται μόνο από την ΚΔΠ.

Δεδομένου ότι κάθε πάροχος ηλεκτρονικής υπηρεσίας διαθέτει ένα ζεύγος κλειδιών για κρυπτογράφηση και αποκρυπτογράφηση δεδομένων, θα πρέπει να κρυπτογραφεί το αντίστοιχο κομμάτι (*Block*) της αλληλουχίας με το δημόσιο κλειδί του ώστε μόνο αυτός να είναι σε θέση να το προσπελάσει, αφού το αποκρυπτογραφήσει με το ιδιωτικό του κλειδί. Με αυτόν τον τρόπο διασφαλίζεται η ιδιωτικότητα των αναγνωριστικών των χρηστών, καθώς η ΚΔΠ μπορεί να αποκρυπτογραφήσει και να προσπελάσει σε μορφή καθαρού κειμένου (*Plain Text*) μόνο το πρώτο τμήμα της.



Σχήμα 4-5: Αλληλουχία Πολλαπλών Αναγνωριστικών σε Σύστημα Ομόσπονδων Ταυτοτήτων

Με βάση τη συγκεκριμένη αλληλουχία, η αρμοδιότητα της διαχείρισης των ψηφιακών ταυτοτήτων των χρηστών μεταφέρεται στην ΚΔΠ, η οποία θα λειτουργεί ως πάροχος ταυτότητας στην ομοσπονδία που θα σχηματίζουν όλοι οι πάροχοι υπηρεσιών. Η εισαγωγή του αναγνωριστικού της ΚΔΠ κρίνεται αναγκαία, ώστε να μπορεί να ταυτοποιείται και να αναγνωρίζεται μοναδικά ο κάθε χρήστης, προκειμένου να αποσταλεί το κατάλληλο τμήμα της αλληλουχίας στον αντίστοιχο πάροχο. Η επιλογή της αξιοποίησης ενός υπάρχοντος αναγνωριστικού για την αρχική ταυτοποίηση των χρηστών στην ΚΔΠ, εγείρει τόσο ζητήματα διασύνδεσης προσωπικών δεδομένων όσο και διαχειριστικές διαδικασίες, καθώς η ΚΔΠ δεν αποτελεί τον υπεύθυνο φορέα έκδοσης και ανάθεσής τους.



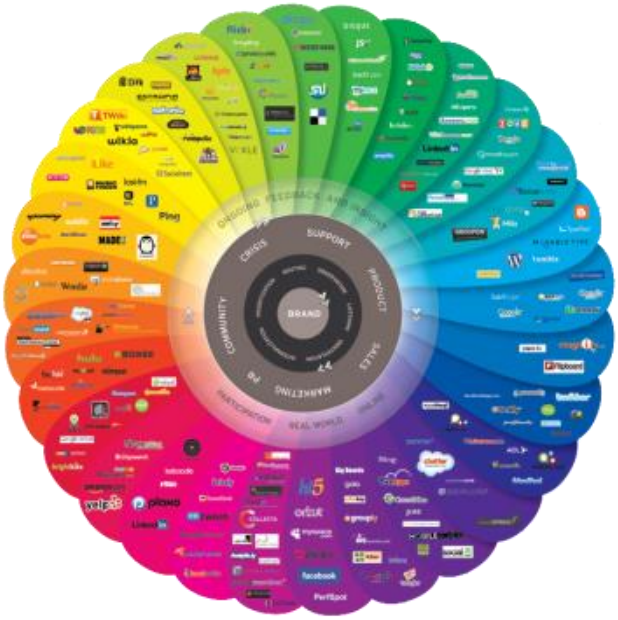
Σχήμα 4-6: Διάγραμμα Λειτουργίας Ομόσπονδων Ταυτοτήτων σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης

Με βάση την προτεινόμενη μέθοδο, ο χρήστης θα αυθεντικοποιείται στην ΚΔΠ και, εφ' όσον ολοκληρώσει επιτυχώς τη συγκεκριμένη διαδικασία, θα αιτείται την παροχή συγκεκριμένης ηλεκτρονικής υπηρεσίας. Στο Σχήμα 4-6 παρουσιάζεται το διάγραμμα λειτουργίας για την παροχή μιας τέτοιας υπηρεσίας, με την αξιοποίηση της συγκεκριμένης μεθόδου. Η υπηρεσία Α απαιτεί, για την ολοκλήρωσή της, παραλαβή συγκεκριμένων στοιχείων από την υπηρεσία Β. Σε ένα μη ομόσπονδο περιβάλλον, ο χρήστης θα έπρεπε να αιτηθεί ξεχωριστά την υπηρεσία Β, να λάβει τις απαιτούμενες πληροφορίες και να τις αποστείλει στην υπηρεσία Α ή να εξουσιοδοτήσει την υπηρεσία Α να ζητήσει τις πληροφορίες από την υπηρεσία Β εκ μέρους του, αποστέλλοντας και το αναγνωριστικό με το οποίο αναγνωρίζεται μοναδικά από τον πάροχό της. Με την αξιοποίηση των ομόσπονδων ταυτοτήτων, όλα τα ψηφιακά αναγνωριστικά του χρήστη βρίσκονται αποθηκευμένα, σε κρυπτογραφημένη μορφή, στην ΚΔΠ. Ο χρήστης αιτείται την παροχή της υπηρεσίας Α στην ΚΔΠ, η οποία τον ταυτοποιεί μέσω του αναγνωριστικού ΚΔΠ και προωθεί στον κατάλληλο πάροχο το αίτημα του χρήστη μαζί το αντίστοιχο κομμάτι, όπου αντιστοιχεί το κρυπτογραφημένο

αναγνωριστικό για τον συγκεκριμένο πάροχο, από την ψηφιακή ταυτότητα του χρήστη. Ο πάροχος υπηρεσίας Α αποκρυπτογραφεί το αναγνωριστικό, προκειμένου να ταυτοποιήσει το χρήστη, και αποστέλλει στην ΚΔΠ αίτημα για παροχή της υπηρεσίας Β για το χρήστη. Η ΚΔΠ αποστέλλει στον πάροχο της υπηρεσίας Β το αντίστοιχο κομμάτι, όπου αντιστοιχεί το κρυπτογραφημένο αναγνωριστικό για τον συγκεκριμένο πάροχο, από την ψηφιακή ταυτότητα του χρήστη, μαζί με το αίτημα από τον πάροχο της υπηρεσίας Α.

4.9 Ηλεκτρονική Διακυβέρνηση 2.0

Η έννοια "Ιστός 2.0 (Web 2.0)" αναφέρεται στο συνδυασμό διαδικτυακών εφαρμογών που διευκολύνουν τη συμμετοχική ανταλλαγή πληροφοριών, τη διαλειτουργικότητα και τη συνεργατικότητα (de Kool & van Wamelen, 2008) και ορίζεται ως "*η φιλοσοφία της αμοιβαίας μεγιστοποίησης της συλλογικής νοημοσύνης και προστιθέμενης αξίας για κάθε συμμετέχοντα, μέσω της δυναμικής ανταλλαγής πληροφοριών και τη δημιουργίας*" (Hoegg et al., 2006). Τέτοιες εφαρμογές περιλαμβάνουν τα blogs, wikis, πλατφόρμες κοινωνικής δικτύωσης, syndication, ομάδες δημόσιου διαλόγου, αυτοματοποιημένη δημιουργία περιεχομένου και ανάλυσης θέματος (Ostergaard & Hvass, 2008). Μία συνολική αποτύπωση όλων αυτών των εφαρμογών, παρουσιάζεται στο Σχήμα 4-7 παρακάτω.



Σχήμα 4-7: Εφαρμογές Ιστού 2.0 (Solis & Thomas, 2013)

Η αξιοποίηση τέτοιων εφαρμογών και η ενσωμάτωσή τους σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης για τη δημιουργία μίας πιο ανοιχτής και συμμετοχικής και διαδραστικής διακυβέρνησης, χαρακτηρίζεται ως "*Ηλεκτρονική Διακυβέρνηση 2.0* (*e-Government 2.0*)" (Meijer et al., 2012) και έχει τη δυνατότητα να αναμορφώσει τη σχέση μεταξύ της Δημόσιας Διοίκησης και των πολιτών, τόσο στη βελτίωση των υπαρχουσών υπηρεσιών όσο και στη χάραξη νέας πολιτικής, προς την κατεύθυνση της Ηλεκτρονικής Δημοκρατίας (Osimo, 2008). Σύμφωνα με (Βέργη, 2009) στην Ηλεκτρονική Διακυβέρνηση 2.0 "*γίνεται μία μετατόπιση δημόσιας πολιτικής προς τη δημιουργία κουλτούρας εξωστρέφειας και διαφάνειας, όπου η κυβέρνηση είναι πρόθυμη να εμπλέξει και να ακούσει τους πολίτες της*" και οι 3 πυλώνες της είναι:

- Η εφαρμογή των εργαλείων και των πρακτικών του Ιστού 2.0 στη διακυβέρνηση,
- Η ανοιχτή πρόσβαση στη δημόσια πληροφορία και
- Η ηγεσία και η πολιτική ώστε να επιτευχθούν οι απαραίτητες αλλαγές στη Δημόσια Διοίκηση.

Ήδη, σε αρκετές χώρες υπάρχουν παραδείγματα αξιοποίησης τέτοιων εφαρμογών στο πλαίσιο της Ηλεκτρονικής Διακυβέρνησης. Ο Πίνακας 4-2 παρακάτω συνοψίζει την αξιοποίησή τους ανά τύπο εφαρμογής και ανά χώρα.

	Blogs	**Ομάδες Συζητήσεων**	**RSS**	**Wikis**
Αυστραλία	●●	●●	●	●
Καναδάς	●	●●●	●●●	●●●
Ολλανδία		●		
Νέα Ζηλανδία	●●●	●		●●
Αγγλία		●		
Η.Π.Α.	●●●●	●	●●	●
Υπόμνημα	● 1-5	●● 6-10	●●● 11 -15	●●●● 16 - 20

Πίνακας 4-2: Πρωτοβουλίες Ηλεκτρονικής Διακυβέρνησης 2.0 (Kujawski, 2013)

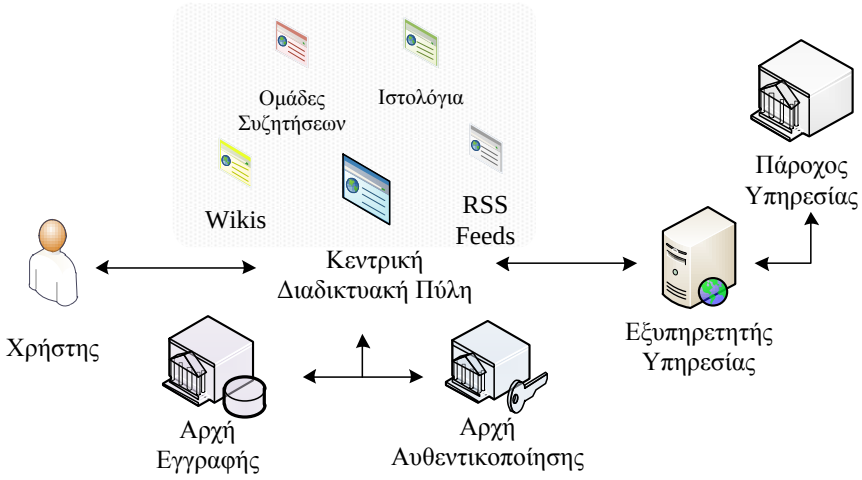
Η ολοκληρωτική μετάβαση σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης 2.0 δεν μπορεί να επέλθει μόνο με την ενσωμάτωση των συγκεκριμένων εφαρμογών, αλλά απαιτεί μία εκ νέου μεταβολή στις σχέσεις της Δημόσιας Διοίκησης με τους πολίτες (Tapscott et al., 2008). Οι

βασικότεροι παράγοντες για την επίτευξη μιας τέτοιας μεταβολής (Coursey & Norris, 2008) (Borins, 2010) είναι:

- *Ηγεσία (Leadership):* Η Δημόσια Διοίκηση θα πρέπει να είναι διατεθειμένη να συμπεριλάβει τους πολίτες στις διαδικασίες διακυβέρνησης και να αξιοποιήσει τη "σοφία του πλήθους (wisdom of the crowd)"
- *Κίνητρα (Incentives)*: Η Δημόσια Διοίκηση θα πρέπει να δώσει τα απαραίτητα κίνητρα στους πολίτες, ώστε να συμμετάσχουν στις διαδικασίες διακυβέρνησης.
- *Εγκαθίδρυση Εμπιστοσύνης (Trust Establishment)*: Ανάπτυξη σχέσεων αμοιβαίας εμπιστοσύνης μεταξύ της Δημόσιας Διοίκησης και των πολιτών.

4.9.1 Προτεινόμενο Μοντέλο Ηλεκτρονικής Διακυβέρνησης 2.0

Στις υφιστάμενες εμπορικές υπηρεσίες – εφαρμογές Ιστού 2.0, η ταυτοποίηση των χρηστών για τη διασφάλιση συγκεκριμένου επιπέδου βεβαιότητας για την ψηφιακή τους ταυτότητα πραγματοποιείται μέσω της αξιοποίησης διαδικασιών αυθεντικοποίησης ονόματος χρήστη - κωδικού πρόσβασης. Για την έκδοση των συγκεκριμένων διακριτικών, ο χρήστης εγγράφεται στην εφαρμογή και σε ορισμένες μόνο περιπτώσεις επιβεβαιώνεται η διεύθυνση ηλεκτρονικού ταχυδρομείου μέσω της αποστολής μηνύματος επαλήθευσης της ηλεκτρονικής διεύθυνσης. Για τους σκοπούς των συγκεκριμένων εφαρμογών, ένα τέτοιο επίπεδο βεβαιότητας για την ταυτότητα του χρήστη μπορεί να είναι επαρκές, αλλά κάτι τέτοιο δεν ισχύει για την παροχή υπηρεσιών ΗΔ. Μπορεί όμως η Δημόσια Διοίκηση να λαμβάνει υπ΄οψιν της την κοινή γνώμη αν δεν μπορεί να γίνει διάκριση μεταξύ των συνεισφορών που αποσκοπούν στην κατάχρηση και τον αποπροσανατολισμό (π.χ. πολλαπλές εγγραφές από τον ίδιο χρήστη) από αυτές που όντως αντιπροσωπεύουν τα αισθήματα του κοινού και εκείνων που αποσκοπούν στην κατάχρηση τα συμπεράσματα και τις διαπιστώσεις; Είναι λοιπόν έκδηλη η ανάγκη για διασφάλιση συγκεκριμένου βαθμού βεβαιότητας στην ψηφιακή ταυτότητα των χρηστών ακόμα και για τις υπηρεσίες Ιστού 2.0 που θα σχετίζονται και θα παρέχονται από τη Δημόσια Διοίκηση. Σε κάθε περίπτωση, όμως, ο βαθμός βεβαιότητας θα πρέπει να είναι ανάλογος με την κρισιμότητα και τη σημασία της παρεχόμενης υπηρεσίας.



Σχήμα 4-8: Αρχιτεκτονική σε Περιβάλλον Ηλεκτρονικής Διακυβέρνησης 2.0

Για την διασφάλιση του απαιτούμενου βαθμού βεβαιότητας, είναι αναγκαίο τόσο οι διαδικασίες της εγγραφής και της αυθεντικοποίησης των χρηστών όσο και η παροχή των υπηρεσιών να πραγματοποιείται από φορείς της Δημόσιας Διοίκησης. Με βάση το μοντέλο και τις λειτουργίες της Κεντρικής Διαδικτυακής Πύλης, προτείνεται η διατήρησή του ως front end για την παροχή και των υπηρεσιών Ιστού 2.0 αξιοποιώντας ταυτόχρονα και τις υπάρχουσες Αρχές Εγγραφής και Αυθεντικοποίησης. Η προτεινόμενη αρχιτεκτονική σε περιβάλλον Ηλεκτρονικής Διακυβέρνησης 2.0 παρουσιάζεται στο ανωτέρω Σχήμα 4-8.

4.9.2 Ψηφιακή Ταυτότητα Χρηστών σε Περιβάλλον Ηλεκτρονικής Διακυβέρνησης 2.0

Προκειμένου να διασφαλιστεί η συμβατότητα με τις υπάρχουσες διαδικασίες ταυτοποίησης και αυθεντικοποίησης των τελικών χρηστών, καθώς και η υπάρχουσα Υποδομή Δημόσιου Κλειδιού, η προτεινόμενη μέθοδος βασίζεται στην έννοια διασύνδεσης των επιμέρους ψηφιακών ταυτοτήτων των τελικών χρηστών, στα πρότυπα της μεθόδου που προτάθηκε στην ενότητα 4.8.3. Μέσω της αξιοποίησης της υπάρχουσας Υποδομής Δημοσίου Κλειδιού και της δημιουργίας μίας αλληλουχίας αναγνωριστικών που θα αποθηκεύεται στην Κεντρική Διαδικτυακή Πύλη, σε συνδυασμό με ένα καινούργιο αναγνωριστικό που θα ανατίθεται από αυτή σε κάθε αλληλουχία. Η συγκεκριμένη αλληλουχία αναγνωριστικών, παρουσιάζεται στο Σχήμα 4-9 παρακάτω, θα έχει προκαθορισμένο μέγεθος που θα καθορίζεται από το σύνολο των παρόχων που προσφέρουν τις υπηρεσίες τους ηλεκτρονικά. Σε κάθε πάροχο θα αντιστοιχίζεται υποχρεωτικά ένα συγκεκριμένο κομμάτι (*Block*) της αλληλουχίας. Δεδομένου ότι κάθε πάροχος ηλεκτρονικής υπηρεσίας διαθέτει

ένα ζεύγος κλειδιών για κρυπτογράφηση και αποκρυπτογράφηση δεδομένων, θα πρέπει να κρυπτογραφεί το αντίστοιχο κομμάτι (block) της αλληλουχίας με το δημόσιο κλειδί του, ώστε μόνο αυτός να είναι σε θέση να το προσπελάσει, αφού το αποκρυπτογραφήσει με το ιδιωτικό του κλειδί. Με αυτόν τον τρόπο διασφαλίζεται η ιδιωτικότητα των αναγνωριστικών των χρηστών, καθώς η ΚΔΠ μπορεί να αποκρυπτογραφήσει και να προσπελάσει σε μορφή καθαρού κειμένου (*Plain Text*) μόνο το πρώτο τμήμα της.

Σχήμα 4-9: Ψηφιακή Ταυτότητα Χρήστη σε Περιβάλλον ΗΔ 2.0

Το αναγνωριστικό "Αναγνωριστικό ΚΠΔ Χρήστη" εισάγεται, ώστε να είναι εφικτή η μοναδική ταυτοποίηση κάθε χρήστη από την ΚΔΠ. Επιπρόσθετα χρησιμεύει και ως μηχανισμός σύνδεσης όλων των επιμέρους τομεακών αναγνωριστικών του χρήστη. Τα επόμενα τμήματα της ακολουθίας αποτελούνται υποχρεωτικά από κρυπτογραφημένα αναγνωριστικά. Ο αριθμός των τμημάτων θα πρέπει να ισούται με τον αριθμό των παρόχων ηλεκτρονικών υπηρεσιών. Σε κάθε πάροχο έχει ανατεθεί ένα συγκεκριμένο τμήμα όπου εκεί αποθηκεύεται, κρυπτογραφημένο, το αντίστοιχο τομεακό αναγνωριστικό. Με αυτόν τον τρόπο η αναζήτηση και αποκρυπτογράφηση γίνεται σε προκαθορισμένο σημείο. Δεδομένου ότι δεν είναι σπάνιο δύο πάροχοι να χρησιμοποιούν το ίδιο τομεακό αναγνωριστικό, θα πρέπει να κρυπτογραφείται δύο φορές στο τμήμα που αντιστοιχεί στον καθένα, με το αντίστοιχο κλειδί κρυπτογράφησης.

4.10 Ηλεκτρονική Διακυβέρνηση και Συστήματα Νεφοϋπολογιστικής

4.10.1 Βασικά Χαρακτηριστικά Συστημάτων Νεφοϋπολογιστικής

Ο όρος "Περιβάλλον Νεφοϋπολογιστικής (*Cloud Computing*)" αναφέρεται στο "*μοντέλο για την διευκόλυνση της διάχυτης (ubiquitous), εύκολης και κατά απαίτηση πρόσβαση σε ένα κοινόχρηστο σύνολο εύκολα παραμετροποιήσεων υπολογιστικών πόρων που μπορούν να διατεθούν και να αξιοποιηθούν με ελάχιστη διαχείριση και αλληλεπίδραση με τον πάροχό τους*" (NIST, 2011). Το μοντέλο αυτό αποτελείται από 5 βασικά χαρακτηριστικά, 3 μοντέλα παροχής υπηρεσιών και 4 μοντέλα ανάπτυξης (NIST, 2011). Τα 5 βασικά χαρακτηριστικά είναι:

- *Αυτό-εξυπηρέτηση κατά απαίτηση (On-demand self-service)*: Ο χρήστης μπορεί να δεσμεύσει μόνος του τους απαιτούμενους υπολογιστικούς πόρους που χρειάζεται χωρίς να απαιτείται ανθρώπινη αλληλεπίδραση με τον πάροχο της υπηρεσίας
- *Ευρεία Πρόσβαση στο Δίκτυο (Broad Network Access)*: Οι υπολογιστικοί πόροι και υπηρεσίες είναι διαθέσιμα μέσω υπαρχόντων υποδομών δικτύου και τεχνολογιών.
- *Διαθεσιμότητα Πόρων (Resource Pooling)*: Οι διαθέσιμοι πόροι διατίθενται για την ταυτόχρονοι εξυπηρέτηση πολλαπλών χρηστών συνδυάζοντας δυναμικά τόσο φυσικούς όσο και εικονικούς πόρους αξιοποιώντας το μοντέλο πολλαπλών μισθωτών (multi-tenant)
- *Ταχεία Ελαστικότητα (Rapid Elasticity)*: Οι πόροι μπορούν να δεσμευτούν και να διατεθούν προς χρήση με γρήγορο και ελαστικό τρόπο ώστε να διασφαλιστεί ο μικρότερος δυνατός χρόνος για τη μετάβαση από "μη διαθέσιμοι" σε "διαθέσιμοι".
- *Μετρούμενη Υπηρεσία (Measured Service)*: Η διάθεση των πόρων μπορεί να οργανώνεται και να βελτιστοποιείται αυτόματα με βάση συγκεκριμένες μετρικές (*Metrics*) και προκαθορισμένα κατώφλια (*Thresholds*)

Τα μοντέλα παροχής υπηρεσιών είναι:

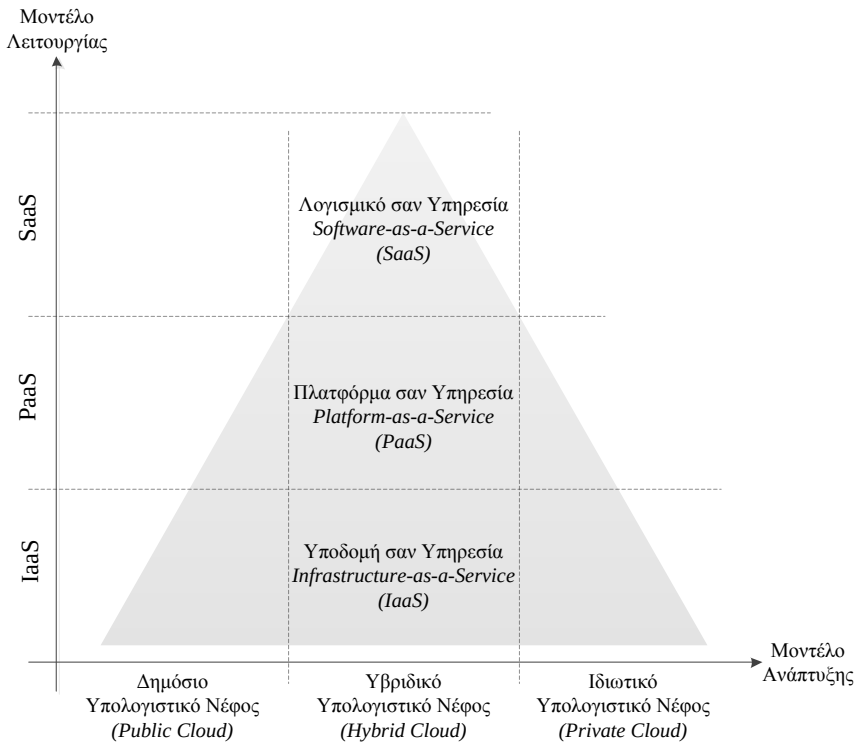
- *Λογισμικό σαν Υπηρεσία (Software as a Service (SaaS))*: Αξιοποίηση και χρήση εφαρμογών που εκτελούνται σε νεφοϋπολογιστικά περιβάλλοντα

- *Πλατφόρμα σαν Υπηρεσία (Platform as a Service (PaaS))*: Αξιοποίηση πλατφόρμων για ανάπτυξη εφαρμογών, συμπεριλαμβανομένου του σχεδιασμού, της εκτέλεσης και της αποσφαλμάτωσης, καθώς και για παροχή λογισμικού σαν υπηρεσία
- *Υποδομή σαν Υπηρεσία (Platform as a Service (PaaS))*: Αξιοποίηση υπολογιστικών υποδομών, όπως επεξεργαστικής ισχύς και χώρου αποθήκευσης σε νεφοϋπολογιστικά περιβάλλοντα

Τα μοντέλα ανάπτυξης είναι:

- *Ιδιωτικό (Private Cloud)*: Η υποδομή λειτουργεί αποκλειστικά και μόνο για έναν οργανισμό.
- *Δημόσιο (Public Cloud)*: Η υποδομή είναι διαθέσιμη στο ευρύ κοινό ή σε μία ευρεία ομάδα οργανισμών.
- *Κοινότητας (Community Cloud)*: Η υποδομή είναι διαθέσιμη σε μία συγκεκριμένη κοινότητα χρηστών.
- *Υβριδικό (Hybrid Cloud)*: Η υποδομή αποτελείς σύνθεση περισσότερων της μιας μοντέλων ανάπτυξης που παραμένουν ως διακριτές οντότητες αλλά διασυνδέονται μεταξύ τους και επιτρέπουν την ανταλλαγή δεδομένων και πληροφοριών (*Intercloud*).

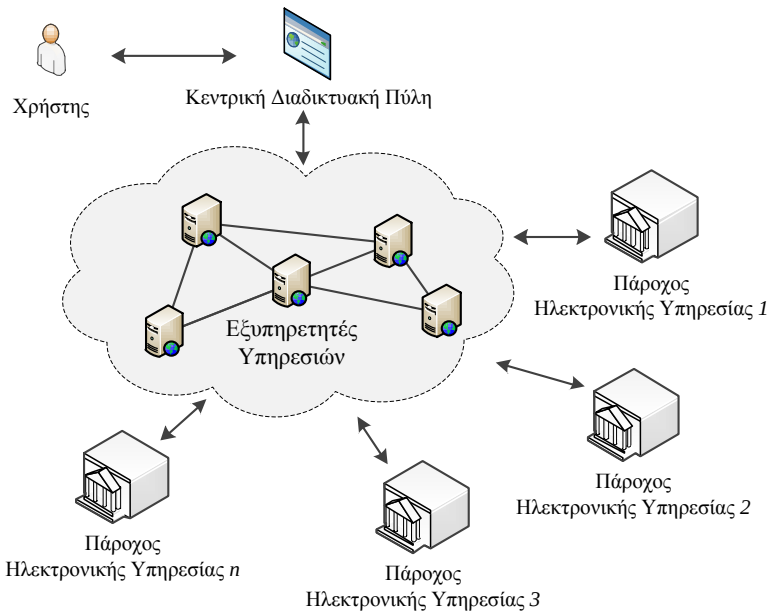
Το Σχήμα 4-10 που ακολουθεί, παρουσιάζει τη συσχέτιση των διαφορετικών μοντέλων ανάπτυξης και λειτουργίας των Συστημάτων Νεφοϋπολογιστικής.



Σχήμα 4-10: Πλαίσιο Λειτουργίας Συστημάτων Νεφοϋπολογιστικής (Rössler, 2010)

4.10.2 Λειτουργία Ηλεκτρονικής Διακυβέρνησης σε Νεφοϋπολογιστικό Περιβάλλον

Η μετάβαση της Δημόσιας Διοίκησης σε νεφοϋπολογιστικό περιβάλλον και η παροχή ηλεκτρονικών υπηρεσιών μέσω αυτού, θα αλλάξει ριζικά τον τρόπο δομής και λειτουργίας των υφιστάμενων IT δομών της. Από την ύπαρξη, διατήρηση και διαχείριση διαφορετικών εξυπηρετητών από κάθε πάροχο υπηρεσίας, θα μεταβεί σε μία δομή όπου δεν είναι διακριτός ο ρόλος των εξυπηρετητών, αναφορικά με τις ηλεκτρονικές υπηρεσίες που παρέχουν στους πολίτες. Τα οφέλη από μία τέτοια μετάβαση θα είναι η κοινή αξιοποίηση των διαθέσιμων υπολογιστικών πόρων, υπηρεσιών, εφαρμογών και δεδομένων από όλους τους δημόσιους φορείς, η βελτίωση της προσβασιμότητας και της διαλειτουργικότητας των παρεχόμενων ηλεκτρονικών υπηρεσιών, καθώς και σημαντική μείωση στο συνολικό κόστος συντήρησης και αναβάθμισης, σε σχέση με τον υπάρχωντα IT εξοπλισμό.



Σχήμα 4-11: Λειτουργία Ηλεκτρονικής Διακυβέρνησης σε Νεφοϋπολογιστικό Περιβάλλον

Παρ' όλα όμως τα αναμενόμενα οφέλη, υπάρχουν και αρκετά ζητήματα θα οποία θα πρέπει να ληφθούν υπ' όψιν, προτού πραγματοποιηθεί μία τέτοια μετάβαση. Σύμφωνα με (Wyld & Maurin, 2009) τα σημαντικότερα ζητήματα που καλείται να αντιμετωπίσει η Δημόσια Διοίκηση είναι:

- *Επιλογή Μοντέλου (Model Selection)*: Επιλογή των κατάλληλων μοντέλων ανάπτυξης και λειτουργίας, με βάση τις απαιτήσεις και τους περιορισμούς, κανονιστικούς και λειτουργικούς, κάθε φορέα, παρόχου, ηλεκτρονικής υπηρεσίας και διαδικασίας,
- *Επεκτασιμότητα (Scalability)*: Οι διαθέσιμοι πόροι θα πρέπει να είναι ευέλικτοι (*Flexible*) και ευκίνητοι (*Agile*) ώστε να προσαρμόζονται στην εκάστοτε ζήτηση,
- *Αξιοπιστία (Reliability):* Διασφάλιση της διαθεσιμότητας (*Availability*) των πόρων,
- *Ασφάλεια των Δεδομένων (Data Security)*: Διασφάλιση συγκεκριμένων επιπέδων ασφάλειας και ιδιωτικότητας για τα δεδομένα και τις παρεχόμενες υπηρεσίες.
- *Ανοικτά Πρότυπα και Διαλειτουργικότητα (Open Standards and Interoperability)*: Αξιοποίηση ανοικτών προτύπων για την διασφάλιση μεγαλύ-

τερου βαθμού διαλειτουργικότητας και αποφυγή εξάρτησης (*Lock-in*) από συγκεκριμένες τεχνολογίες και πρότυπα,

- *Πιθανά Νομικά Προβλήματα (Potential Legal Issues)*: Διασφάλιση της νομικής υπόστασης των ηλεκτρονικά παρεχόμενων υπηρεσιών και διαδικασιών μέσα από νεφοϋπολογιστικό περιβάλλον,
- *Απόδοση Επενδύσεων (Return on Investment)*: Υπολογισμός και πρόβλεψη απόσβεσης της αρχικής επένδυσης για τη μετάβαση και
- *Συντονισμός (Coordination):* Στρατηγικός σχεδιασμός και επίβλεψη όλων των επιμέρους ανεπτυγμένων συστημάτων.

4.10.3 Ασφάλεια και Ιδιωτικότητα σε Νεφοϋπολογιστικό Περιβάλλον

Ένας από τους βασικότερους ανασταλτικούς παράγοντες για την παροχή ηλεκτρονικών υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, που αξιοποιούν συστήματα Νεφοϋπολογιστικής, είναι η ασφάλεια των δεδομένων και των παρεχόμενων υπηρεσιών σε όλες τις εκφάνσεις της. Όπως αναφέρθηκε και στην ενότητα 3.4.1, οι βασικές απαιτήσεις ασφάλειας και ιδιωτικότητας σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης σχετίζονται με απειλές που ενδέχεται να προέλθουν από:

- Μη εξουσιοδοτημένη πρόσβαση
  - σε πληροφορία ή
  - στην παρεχόμενη υπηρεσία
- Αντιποίηση αρχής
  - εξουσιοδοτημένου χρήστη
  - υπηρεσίας
- Παραβίαση της ιδιωτικότητας και παράνομη πρόσβαση ή χρήση των δεδομένων προσωπικού χαρακτήρα
- Άρνηση παροχής υπηρεσίας

Ανάλογα, όμως, με το μοντέλο ανάπτυξης και το μοντέλο λειτουργίας που θα επιλεγεί για την παροχή των ηλεκτρονικών υπηρεσιών, το επίπεδο του κινδύνου διαφέρει σημαντικά για καθεμία από τις παραπάνω απειλές. Σύμφωνα με την αναφορά που εξέδωσε ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA, 2009), οι σημαντικότερες κατηγο-

ρίες κινδύνων για τον χρήστη υπηρεσιών νεφοϋπολογιστικής, που δυνητικά θα μπορούσε να είναι η Δημόσια Διοίκηση, είναι:

- *Απώλεια Διακυβέρνησης (Loss of Governance)*: Ο χρήστης εκχωρεί αναγκαστικά τον έλεγχο στον πάροχο των συστημάτων νεφοϋπολογιστικής και δεν μπορεί πλέον να έχει τον απόλυτο έλεγχο για ζητήματα που σχετίζονται με την ασφάλεια και την ιδιωτικότητα των δεδομένων και τον υπηρεσιών.
- *Εξάρτηση (Lock-In)*: Εξαιτίας της έλλειψης καθολικά αποδεκτών και αξιοποιήσιμων προτύπων και τεχνολογιών, ο πάροχος δεν μπορεί να εγγυηθεί την φορητότητα των δεδομένων και των υπηρεσιών
- *Αποτυχία Απομόνωσης (Failure Isolation)*: Η μίσθωση κοινόχρηστων πόρων μπορεί να εισαγάγει επιπρόσθετους κινδύνους σχετικά με την ασφάλεια και την ιδιωτικότητα των δεδομένων και των υπηρεσιών του χρήστη, σε περίπτωση απώλειας των μηχανισμών απομόνωσής τους από τους υπόλοιπους κοινόχρηστους πόρους
- *Κίνδυνοι Συμμόρφωσης (Compliance Risks)*: Η μετάβαση σε συστήματα νεφοϋπολογιστικής μπορεί να αποτελέσει ανασταλτικό παράγοντα για την επίτευξη συμμόρφωσης σε συγκεκριμένα πρότυπα ασφάλειας
- *Προστασία των Δεδομένων (Data Protection)*: Είναι δύσκολο για έναν χρήστη να ελέγξει την αποτελεσματικότητα των μεθόδων και των διαδικασιών που αξιοποιούνται για την προστασία των δεδομένων.

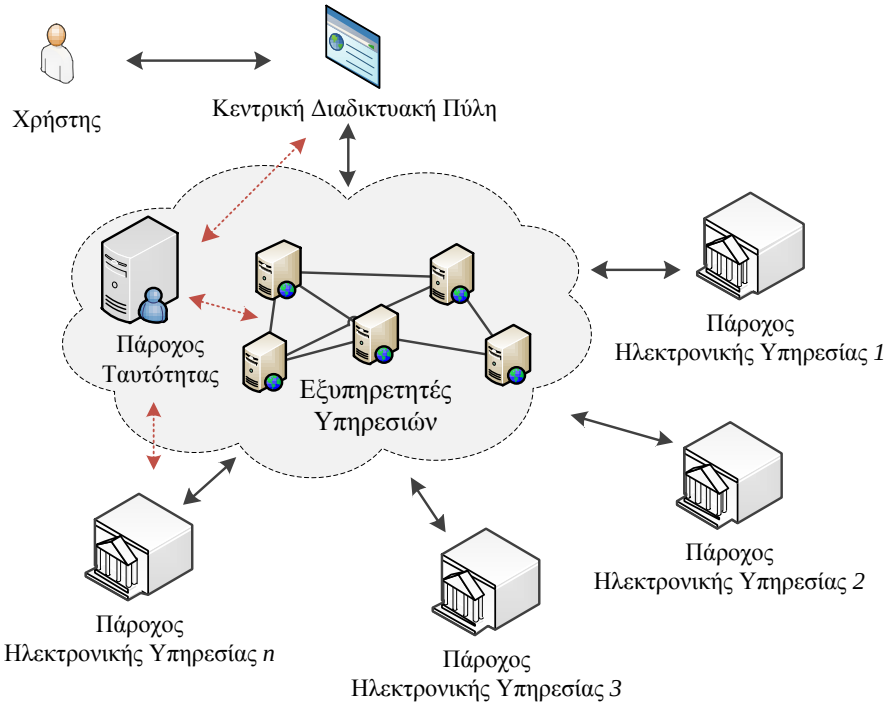
Στους παραπάνω κινδύνους θα πρέπει να προστεθεί και η έλλειψη νομικού και κανονιστικού πλαισίου βάσει του οποίου θα καθορίζεται το πλαίσιο παροχής υπηρεσιών Ηλεκτρονικής Διακυβέρνησης με τη χρήση συστημάτων νεφοϋπολογιστικής. Προς την κατεύθυνση της δημιουργίας ενός ολοκληρωμένου πλαισίου ασφάλειας το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας της Αμερικής προτείνει την ύπαρξη των κάτωθι διακριτών φάσεων (NIST, 2011):

- Κατηγοριοποίηση των υπηρεσιών ασφάλειας (*Service security categorization*),
- Επιλογή ελέγχων ασφάλειας (*Security controls selection*),
- Εφαρμογή ελέγχων ασφάλειας (*Security controls implementation*),
- Αξιολόγηση ελέγχων ασφάλειας (*Security controls assessment*),
- Εξουσιοδότηση υπηρεσιών (*Service Authorization*) και

- Παρακολούθηση αποτελεσματικότητας ελέγχων ασφάλειας (*Monitoring the effectiveness of security controls*)

4.10.4 Διαχείριση Ψηφιακών Ταυτοτήτων σε Νεφοϋπολογιστικό Περιβάλλον

Αντίστοιχα με την ασφάλεια και την ιδιωτικότητα σε νεφοϋπολιγιστικά περιβάλλοντα όπου η επιλογή μοντέλου ανάπτυξης και λειτουργίας επηρεάζει άμεσα το επίπεδο κινδύνου, το ίδιο συμβαίνει και κατά τη διαχείριση των ψηφιακών ταυτοτήτων των τελικών χρηστών (Chow et al., 2009).



Σχήμα 4-12: Πάροχος Ταυτότητας σε Νεφοϋπολογιστικό Περιβάλλον

Δεδομένης της απαίτησης για διαλειτουργικότητα, η ύπαρξη ενός κεντρικού παρόχου ταυτότητας μπορεί να καταστήσει δυνατή την αλληλεπίδραση των διαφόρων παρόχων, στα πρότυπα μιας ομόσπονδης αρχιτεκτονικής, όπως αυτή παρουσιάστηκε στην ενότητα 4.8.2

ΚΕΦΑΛΑΙΟ 5 - ΠΛΑΙΣΙΟ ΨΗΦΙΑΚΗΣ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ

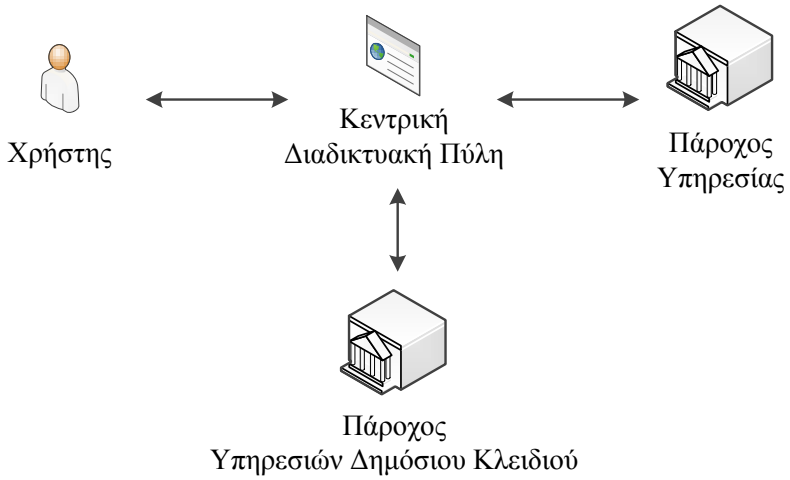
Στο παρόν κεφάλαιο παρουσιάζεται και προτείνεται ένα ολοκληρωμένο Πλαίσιο Ψηφιακής Αυθεντικοποίησης, που αποσκοπεί στη θέσπιση κανόνων και οδηγιών για την ιεράρχηση της κρισιμότητας κάθε ηλεκτρονικής υπηρεσίας, και την επιλογή των μηχανισμών αυθεντικοποίησης και εγγραφής, με τρόπο σαφή, απλό, μεθοδικό και τεκμηριωμένο. Οι κανόνες και οι οδηγίες του βασίζονται στο ισχύον εθνικό νομικό και κανονιστικό πλαίσιο για την προστασία των προσωπικών και ευαίσθητων προσωπικών δεδομένων, καθώς και στην προάσπιση της ιδιωτικότητας των πολιτών.

5.1 Σκοπός του Πλαισίου Ψηφιακής Αυθεντικοποίησης

Στο πλαίσιο του εθνικού έργου «eGIF: Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Πρότυπα Διαλειτουργικότητας: Πλαίσιο Ψηφιακής Αυθεντικοποίησης» (e-GIF, 2009), εκπονήθηκε μελέτη για τη σχεδίαση του Πλαισίου Ψηφιακής Αυθεντικοποίησης (ΠΨΑ) (ΚτΠ, 2009). Το συγκεκριμένο έργο εντάσσεται στο συνολικό σχεδιασμό της Ελληνικής Δημόσιας Διοίκησης για την παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης σε φορείς, επιχειρήσεις και πολίτες. Σκοπός του ΠΨΑ είναι να υποστηρίξει και να καθοδηγήσει τους φορείς της Δημόσιας Διοίκησης που παρέχουν ή σχεδιάζουν να παρέχουν υπηρεσίες ηλεκτρονικής διακυβέρνησης, στην επιλογή των κατάλληλων μηχανισμών αυθεντικοποίησης και στον καθορισμό των διαδικασιών εγγραφής και ταυτοποίησης των χρηστών. Η υιοθέτηση των οδηγιών και κατευθύνσεων του ΠΨΑ έχει ως στόχο τη βελτίωση του συνολικού επιπέδου ασφάλειας των παρεχόμενων υπηρεσιών από φορείς της Δημόσιας Διοίκησης, επιτρέποντας τη βελτίωση της συνολικής λειτουργίας της και την εναρμόνισή τους με την ευρωπαϊκή πολιτική και τις αντίστοιχες κατευθύνσεις.

Η γενική αρχιτεκτονική του ΠΨΑ παρουσιάζεται στο Σχήμα 5-1 παρακάτω. Συνοπτικά, οι δημόσιοι φορείς προσφέρουν τις υπηρεσίες τους μέσω της Κεντρικής Διαδικτυακής Πύλης (ΚΔΠ), αφού πρώτα δηλώσουν τις απαιτήσεις τους για κάθε υπηρεσία (επίπεδο εμπιστοσύνης, αυθεντικοποίησης, εγγραφής), καθώς επίσης και τα απαιτούμενα δικαιολογητικά που πρέπει οι χρήστες να υποβάλουν κατά τη διαδικασία εγγραφής. Οι τελικοί χρήστες, αφού εγγραφούν στην ηλεκτρονική υπηρεσία μέσω της ΚΔΠ, μπορούν να αιτηθούν την παροχή και να αξιοποιήσουν τις

προσφερόμενες ηλεκτρονικές υπηρεσίες. Σε κάθε περίπτωση, όμως, θα πρέπει πρώτα να ελεγχθεί και διαπιστωθεί η ορθότητα της ηλεκτρονικής τους ταυτότητας.



Σχήμα 5-1: Γενική Αρχιτεκτονική ΠΨΑ

Η πλειονότητα των ηλεκτρονικών υπηρεσιών που προσφέρονταν, πριν την εφαρμογή του ΠΨΑ, από την Δημόσια Διοίκηση, αξιοποιούσαν ως μέθοδο ταυτοποίησης και αυθεντικοποίησης τη χρήση ονομάτων χρηστών (*Username*) και συνθηματικών (*Password*) για την επιβεβαίωση της ψηφιακής ταυτότητας των χρηστών, ενώ ακολουθούνταν ανάλογα απλουστευμένες διαδικασίες εγγραφής. Η συγκεκριμένη μέθοδος αυθεντικοποίησης δε λαμβάνει υπόψη την κρισιμότητα των υπηρεσιών, αναφορικά με τις επιπτώσεις που είναι δυνατόν να προκληθούν στο φορέα και στο χρήστη σε περίπτωση εκδήλωσης κάποιου περιστατικού ασφάλειας. Το ΠΨΑ, μέσα από τη θέσπιση κανόνων και οδηγιών – οι οποίοι βασίζονται στο ισχύον νομικό και κανονιστικό πλαίσιο για την προστασία των προσωπικών και ευαίσθητων προσωπικών δεδομένων, καθώς και στην προστασία της ιδιωτικότητας του πολίτη – απλοποιεί την ιεράρχηση της κρισιμότητας κάθε ηλεκτρονικής υπηρεσίας και συνεπώς την επιλογή των ενδεδειγμένων μηχανισμών αυθεντικοποίησης, τηρώντας την "Αρχή της Αναλογικότητας" (*The principle of Proportionality*).

5.1.1 Πεδίο Εφαρμογής του Πλαισίου Ψηφιακής Αυθεντικοποίησης

Το ΠΨΑ απευθύνεται σε όλους τους φορείς της Δημόσιας Διοίκησης, οι οποίοι διαθέτουν, αναπτύσσουν ή σχεδιάζουν να αναπτύξουν διαδικτυακό τόπο με σκοπό να παρέχουν πλη-

ροφορίες και υπηρεσίες σε πολίτες, επιχειρήσεις και άλλους φορείς. Αναλυτικότερα, το Πλαίσιο απευθύνεται σε:

- Υπουργεία και Γενικές Γραμματείες,
- Περιφέρειες,
- Νομαρχιακές Αυτοδιοικήσεις,
- Οργανισμούς Τοπικής Αυτοδιοίκησης,
- Εποπτευόμενους φορείς του Δημόσιου Τομέα ,
- Ανεξάρτητες Αρχές και
- τους υπόλοιπους φορείς του Δημόσιου Τομέα όπως αυτός ορίζεται βάσει του Ν. 2527/97, άρθρο 1.

Επιπρόσθετα, απευθύνεται σε οργανισμούς του ευρύτερου Δημόσιου και του Ιδιωτικού Τομέα, οι οποίοι διαδραματίζουν σημαντικό ρόλο στην ανάπτυξη και παροχή ηλεκτρονικών υπηρεσιών μέσω δημόσιων διαδικτυακών τόπων προς πολίτες, επιχειρήσεις και άλλους φορείς, και αναλυτικότερα:

- Δημόσιες Επιχειρήσεις Κοινής Ωφέλειας,
- Τραπεζικούς και Χρηματοπιστωτικούς Οργανισμούς και
- Επιχειρήσεις Πληροφορικής που δραστηριοποιούνται στην ανάπτυξη λογισμικού και την παροχή συναφών υπηρεσιών για φορείς της Δημόσιας Διοίκησης.

5.1.2 Θέματα Ιδιωτικότητας στις Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης

Η αξιοποίηση υπηρεσιών ηλεκτρονικής διακυβέρνησης απαιτεί συλλογή και επεξεργασία διαφορετικού είδους πληροφοριών, όπως προσωπικών δεδομένων, των οποίων η προστασία, επεξεργασία και μη αποκάλυψη και δημοσιοποίηση αποτελεί βασική κανονιστική απαίτηση, σύμφωνα με τις ειδικότερες προϋποθέσεις και εγγυήσεις της σχετικής νομοθεσίας (ν. 2472/97), που πρέπει να εκπληρώνεται από τις υπηρεσίες ηλεκτρονικής διακυβέρνησης. Η συνταγματική και έννομη τάξη αναγνωρίζει την ιδιωτικότητα των πληροφοριών (*Informational privacy*), ως το δικαίωμα και τη δυνατότητα του ατόμου να γνωρίζει, να ελέγχει και καταρχήν να προσδιορίζει τη χρήση των προσωπικών πληροφοριών του από άλλες οντότητες, ιδιώτες και κράτος. Ως ιδιωτικότητα ορίζεται η μη αποκάλυψη προσωπικών πληροφοριών σε μη εξουσιοδοτημένες οντότητες, η οποία αποτελεί βασική παράμετρο της σχετικής νομοθεσίας που αναγνωρίζεται ρητά (άρθρο 10 Ν.2472/97), ενώ η παραβίασή της τιμωρείται και με ποινικές κυρώσεις (άρθρο 22 § 4 Ν.

2472/97). Το δικαίωμα στην ιδιωτικότητα αναφέρεται στη δυνατότητα ελέγχου της χρήσης των προσωπικών πληροφοριών.

5.1.3 Κατηγορίες Δεδομένων

Οι τρεις κατηγορίες δεδομένων, με βάση την απαίτηση για προάσπιση της ιδιωτικότητάς τους, που μπορούν να αξιοποιηθούν για την ολοκλήρωση κάθε ηλεκτρονικής υπηρεσίας είναι τα:

- Δημόσια (προσπελάσιμα - διαθέσιμα) δεδομένα,
- Προσωπικά δεδομένα και
- Ευαίσθητα (προσωπικά) δεδομένα.

Ως δημόσια προσπελάσιμα – διαθέσιμα δεδομένα προσδιορίζονται τα δεδομένα που δεν αποτελούν ευαίσθητες ή προσωπικές πληροφορίες. Ως τέτοια νοούνται τα ανώνυμα στατιστικά στοιχεία, το πληροφοριακό υλικό των φορέων της Δημόσιας Διοίκησης, οι πράξεις νομοθετικού περιεχομένου κλπ. Τα απλά στατιστικά δεδομένα δεν είναι εξ ορισμού και δημόσια. Μόνο εφόσον πιστοποιηθεί ότι δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων, και μόνο τότε, μπορούμε να τα διαχειριζόμαστε ως δημόσια διαθέσιμη πληροφορία.

Ως δεδομένα προσωπικού χαρακτήρα ή προσωπικά δεδομένα νοούνται οι πληροφορίες που αναφέρονται στο υποκείμενο των δεδομένων. Αναφέρονται δηλαδή στο φυσικό πρόσωπο το οποίο αφορούν και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, μπορεί δηλαδή να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική (άρθρο 2α σε συνδυασμό με άρθρο 2γ του Ν. 2472/97). Τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν είναι δυνατός ο προσδιορισμός των υποκειμένων δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα. Στον όρο "προσωπικά δεδομένα" περιλαμβάνονται και αυτά που συνήθως χρησιμοποιούνται για τον προσδιορισμό της ταυτότητας του προσώπου (μοναδικά αναγνωριστικά). Ως στοιχεία που δηλώνουν την ταυτότητα ενός προσώπου έχουν γίνει αποδεκτά και στοιχεία που αποδίδονται σε πρόσωπα ή επιλέγονται από αυτό (π.χ. κωδικός αναγνώρισης ή πρόσβασης, αριθμός PIN κ.α.).

Ως ευαίσθητα προσδιορίζονται σαφώς στο άρθρο 2β του Ν. 2472/97 τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική

πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

Στον Πίνακας 5-1, συνοψίζονται οι κατηγορίες των δεδομένων καθώς και οι απαιτήσεις τους αναφορικά με την προάσπιση της ιδιωτικότητάς τους.

Κατηγορία Δεδομένων	**Περιγραφή**
Δημόσια Διαθέσιμα Δεδομένα	Σε αυτή τη κατηγορία περιλαμβάνονται τα δεδομένα που είναι δημοσίως προσπελάσιμα και δεν περιέχουν προσωπικές πληροφορίες
Προσωπικά Δεδομένα	Σε αυτή τη κατηγορία δεδομένων περιλαμβάνονται όλα εκείνα τα στοιχεία που σχετίζονται με ένα πρόσωπο όπως Όνομα, Επίθετο, ημερομηνία γέννησης, Αριθμός Φορολογικού Μητρώου (ΑΦΜ), εναλλακτικά αναγνωριστικά, διεύθυνση αλληλογραφίας, ηλεκτρονική διεύθυνση αλληλογραφίας. Επισημαίνεται ότι και ως προς αυτά τα δεδομένα δεν πρέπει να γίνεται καμία χρήση χωρίς να υπάρχει «εξουσιοδότηση» που εν προκειμένω νοείται εν γένει ως νομική βάση της επεξεργασίας (δηλ. νόμος, δημόσιο συμφέρον, συγκατάθεση κλπ.).
Ευαίσθητα Δεδομένα	Σε αυτή την κατηγορία περιλαμβάνονται τα δεδομένα που ορίζει ο Ν. 2472/97 στο άρθρο 2β και την επεξεργασία των οποίων ρυθμίζει στο άρθρο 7 και 7 Α .

Πίνακας 5-1: Κατηγοριοποίηση Δεδομένων με βάση την Απαίτηση για Ιδιωτικότητα

5.1.4 Υποχρεώσεις Δημόσιας Διοίκησης

Οι βασικές υποχρεώσεις της Διοίκησης σχετικά με τη διασφάλιση της Ιδιωτικότητας, όταν παρέχονται υπηρεσίες ηλεκτρονικής διακυβέρνησης με χρήση δεδομένων προσωπικού χαρακτήρα, είναι:

- Κατά τη συλλογή και επεξεργασία δεδομένων, θα πρέπει να λαμβάνεται πρόνοια, ώστε να υπάρχει σαφής προσδιορισμός και διαχωρισμός των δεδομένων προσωπικού και στατιστικού χαρακτήρα.

- Θα πρέπει να διασφαλίζεται, με διαδικασίες ανωνυμοποίησης/ πολλαπλής κωδικοποίησης, ότι από τα δεδομένα στατιστικού χαρακτήρα δεν είναι δυνατός ο προσδιορισμός της ταυτότητας των φυσικών προσώπων.
- Με εγκυκλίους και άλλα μέσα ενημέρωσης-εκπαίδευσης θα πρέπει να καταστούν γνωστές και σαφείς στους δημόσιους υπαλλήλους οι κατηγορίες των ευαίσθητων δεδομένων, για να αποφευχθεί σχετική σύγχυση (π.χ. παρατηρείται σχετική σύγχυση μεταξύ των δεδομένων που αφορούν φυλετική ή εθνική προέλευση (φυλετική ή εθνική μειονότητα), που συνιστούν ευαίσθητα δεδομένα, και αυτών που αφορούν την ιθαγένεια, που συνιστούν απλά δεδομένα).

Σε περίπτωση προσφυγής σε εξωτερικούς ιδιωτικούς φορείς για την αποθήκευση και πρόσβαση σε προσωπικά δεδομένα χρήστη:

- Θα πρέπει να περιλαμβάνονται στη σχετική σύμβαση όροι για τη συλλογή και επεξεργασία δεδομένων.
- Θα ήταν χρήσιμο ένα ενιαίο πρότυπο συμβατικών όρων που θα προσδιορίζουν τις υποχρεώσεις των τρίτων ως προς τη συλλογή και χρήση προσωπικών δεδομένων. Οι πρότυποι όροι θα μπορούσαν να χρησιμοποιηθούν από τις υπηρεσίες με τις αναγκαίες κατά περίπτωση προσαρμογές.
- Σε περίπτωση ανάθεσης της παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης σε τρίτους, εφόσον οι υπηρεσίες αυτές προϋποθέτουν ή/και συνεπάγονται συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα, η αναλυτική περιγραφή και ποιότητα των πολιτικών εφαρμογής των κανόνων προστασίας και των πολιτικών/ μέτρων ασφάλειας, θα έπρεπε να αναχθεί σε κριτήριο επιλογής αναδόχου ή/και όρο ανάθεσης.

5.2 Επίπεδα Εμπιστοσύνης

Ο καθορισμός του βαθμού κρισιμότητας των δεδομένων εξαρτάται κατά κύριο λόγο από τις επιπτώσεις που μπορεί να προκύψουν:

- για το χρήστη ή / και το φορέα που προσφέρει την υπηρεσία, λόγω της αποκάλυψης ή «παράνομης και αθέμιτης» χρήσης των δεδομένων,
- στην ιδιωτικότητα του ατόμου.

Κατά την ανάλυση και τον προσδιορισμό των Επιπέδων Εμπιστοσύνης, λαμβάνονται υπόψη τα παραπάνω κριτήρια που αναφέρονται τόσο στο χαρακτηρισμό των δεδομένων όσο και στην εκτίμηση της πιθανότητας επέλευσης βλάβης (αποκάλυψη εμπιστευτικών δεδομένων, μη εξουσιοδοτημένη τροποποίηση, μη διαθεσιμότητα δεδομένων, αποποίηση) είτε αυτή οφείλεται σε παράνομη ή αθέμιτη χρήση είτε όχι. Συνεπώς, όσο πιο κρίσιμη θεωρείται μια υπηρεσία, τόσο μεγαλύτερο επίπεδο εμπιστοσύνης απαιτείται για την ορθότητα και εγκυρότητα των στοιχείων που επιδεικνύει ή προσκομίζει ο χρήστης για τη χρήση των υπηρεσιών ηλεκτρονικής διακυβέρνησης. Σε κάθε περίπτωση, το Επίπεδο Εμπιστοσύνης που επιλέγεται για μια υπηρεσία, θα πρέπει να στοχεύει στα ακόλουθα:

- Στην ελευθερία της πληροφόρησης και ενημέρωσης των πολιτών για θέματα δημόσιας διαβούλευσης,
- Στην εκπλήρωση του δικαιώματος συμμετοχής στην κοινωνία της πληροφορίας,
- Στη διαφύλαξη του δικαιώματος κάθε πολίτη για αποτελεσματική και ασφαλή διεκπεραίωση των συναλλαγών του με τους δημόσιους φορείς και
- Στη διαφύλαξη και ορθή διαχείριση των προσωπικών δεδομένων κάθε πολίτη

5.2.1 Προσδιορισμός Επιπέδων Εμπιστοσύνης

Η "*εμπιστοσύνη*", ερμηνεύεται ως "*η πίστη στην αξιοπιστία, εντιμότητα, αξία ή ικανότητα κάποιας οντότητας*". Υπό το πρίσμα του ΠΨΑ, ως Επίπεδο Εμπιστοσύνης μπορεί να θεωρηθεί "*Ο βαθμός βεβαιότητας που έχει μια υπηρεσία για την ορθότητα τόσο της ηλεκτρονικής οντότητας ενός πολίτη που επιθυμεί να διεκπεραιώσει ηλεκτρονικά μια συναλλαγή, όσο και των δεδομένων που απαιτούνται για την επιτυχή ολοκλήρωση της συναλλαγής, λαμβάνοντας υπόψη και την κρισιμότητα των δεδομένων αυτών (απλά, προσωπικά, ευαίσθητα)*".

Το κάθε Επίπεδο Εμπιστοσύνης προσδιορίζει όχι μόνο το βαθμό βεβαιότητας ότι ο πολίτης που επιδεικνύει συγκεκριμένου τύπου διαπιστευτήρια, είναι πράγματι αυτός που ισχυρίζεται ότι είναι, με κύριο στόχο να εξασφαλιστεί η δημιουργία εμπιστοσύνης μεταξύ της υπηρεσίας και του χρήστη για τη διεκπεραίωση της συναλλαγής, αλλά και ότι αξιοποιούνται οι κατάλληλοι μηχανισμοί ασφάλειας για την προστασία των δεδομένων που απαιτούνται, με βάση την κρισιμότητά τους. Το κάθε επίπεδο διαμορφώνεται ανάλογα με την αξία των συναλλαγών, την κρισιμότητα των δεδομένων που χρησιμοποιούνται, των άμεσων ή έμμεσων επιπτώσεων που μπορεί να προ-

κύψουν από την εκδήλωση επιθέσεων, καθώς επίσης και από την αντίστοιχη επιρροή του θεσμικού πλαισίου. Τα Επίπεδα Εμπιστοσύνης για τις υπηρεσίες ηλεκτρονικής διακυβέρνησης, σύμφωνα με τα παραπάνω κριτήρια, περιγράφονται στις επόμενες υποενότητες.

5.2.2 Επίπεδο Εμπιστοσύνης 0

Στο Επίπεδο Εμπιστοσύνης 0 εντάσσονται υπηρεσίες που αξιοποιούν δημόσια προσπελάσιμες πληροφορίες και έχουν ως κύριο στόχο την πληροφόρηση των πολιτών γύρω από συγκεκριμένα θέματα. Οι υπηρεσίες αυτές δεν απαιτούν:

- τη χρήση ή ανταλλαγή οποιουδήποτε τύπου προσωπικών ή οικονομικών δεδομένων,
- κάποιο βαθμό βεβαιότητας για την ορθότητα της ηλεκτρονικής οντότητας ενός χρήστη.

Στο παρόν επίπεδο δεν υπάρχουν ιδιαίτερες επιπτώσεις από οποιαδήποτε παράνομη ή αθέμιτη χρήση των δεδομένων που αξιοποιούν οι ηλεκτρονικές υπηρεσίες. Η μοναδική πιθανή επίπτωση είναι η λανθασμένη πληροφόρηση του χρήστη, σε περίπτωση που δεν τηρούνται τα στοιχειώδη μέτρα ασφάλειας και κάποιος κακόβουλος χρήστης υποδυθεί την υπηρεσία. Οι μοναδικές απαιτήσεις είναι η ακεραιότητα των μεταδιδόμενων δεδομένων, η αυθεντικοποίηση της υπηρεσίας και η διαθεσιμότητά της.

5.2.3 Επίπεδο Εμπιστοσύνης 1

Στο Επίπεδο Εμπιστοσύνης 1 εντάσσονται υπηρεσίες που απαιτούν ανταλλαγή δεδομένων μικρής ή ελάχιστης κρισιμότητας, όπως για παράδειγμα το ονοματεπώνυμο ή η διεύθυνση ηλεκτρονικού ταχυδρομείου για τη διεκπεραίωση μιας συναλλαγής. Σε αντίθεση με το επίπεδο εμπιστοσύνης 0, στο συγκεκριμένο επίπεδο η ηλεκτρονική υπηρεσία απαιτεί κάποιο μικρό βαθμό βεβαιότητας για την ορθότητα της ηλεκτρονικής οντότητας του πολίτη, ώστε να αποδεικνύεται η ορθότητα την στοιχείων που υποβάλλονται. Οι επιπτώσεις που μπορεί να προκληθούν από τη λανθασμένη επεξεργασία και διαχείριση των δεδομένων είναι κυρίως δευτερεύουσας σημασίας και αφορούν κυρίως στην αποκάλυψη προσωπικών δεδομένων, όπως ηλεκτρονικό μήνυμα, τηλέφωνο κ.λπ.

Για το συγκεκριμένο επίπεδο, το ΠΨΑ προτείνει τη λήψη ορισμένων μέτρων ασφάλειας, που έχουν ως στόχο την προστασία των δεδομένων που ανταλλάσσονται και την ελαχιστοποί-

ηση της πιθανότητας εμφάνισης κάποιας απειλής. Οι απαιτήσεις ασφάλειας του Επιπέδου Εμπιστοσύνης 1 περιλαμβάνουν την ακεραιότητα των μεταδιδόμενων δεδομένων και την εμπιστευτικότητα των μεταδιδόμενων προσωπικών δεδομένων, τη μη αποποίηση παραλαβής ενός αιτήματος του πολίτη από τη διοίκηση, τη μη αποποίηση αποστολής των απαντήσεων από αρμόδιο υπάλληλο που διεκπεραίωσε το σχετικό αίτημα, προς τον πολίτη, καθώς και (σε ορισμένες περιπτώσεις) τη μη αποποίηση αποστολής αιτήσεων ή/και παραλαβής απαντήσεων της διοίκησης, από τον πολίτη, την αυθεντικοποίηση και τη διαθεσιμότητα της υπηρεσίας.

5.2.4 Επίπεδο Εμπιστοσύνης 2

Στο Επίπεδο Εμπιστοσύνης 2 εντάσσονται υπηρεσίες που απαιτούν ανταλλαγή προσωπικών δεδομένων τα οποία δεν έχουν χαρακτηριστεί ως ευαίσθητα, όπως για παράδειγμα στοιχεία που αφορούν την οικογενειακή κατάσταση του χρήστη, ημερομηνία γέννησης, φύλο κ.λπ. Επίσης, με βάση την ισχύουσα νομοθεσία, τα οικονομικά δεδομένα που δεν καλύπτονται από το φορολογικό απόρρητο, εντάσσονται στα προσωπικά δεδομένα. Στο συγκεκριμένο επίπεδο, ο βαθμός βεβαιότητας για την ορθότητα της ηλεκτρονικής οντότητας που αξιοποιεί την υπηρεσία, χαρακτηρίζεται ως μέτριος, καθώς πρέπει να εξασφαλίζεται ότι οι υπηρεσίες προσφέρονται μόνο σε εξουσιοδοτημένες οντότητες. Οι επιπτώσεις, που μπορεί να προκληθούν από την εμφάνιση κάποιων επιθέσεων και απειλών ή τη λανθασμένη επεξεργασία και διαχείριση των δεδομένων, είναι σημαντικές και αφορούν κυρίως στη δημοσιοποίηση προσωπικών στοιχείων (μη ευαίσθητων) που συμπεριλαμβάνονται σε πιστοποιητικά και βεβαιώσεις όπως οικογενειακής κατάστασης, πιστοποιητικό γέννησης κ.λπ., χωρίς τη γνώση ή έγκριση του χρήστη, είτε σε μη εξουσιοδοτημένα άτομα είτε στο ευρύ κοινό.

Οι απαιτήσεις ασφάλειας του Επιπέδου Εμπιστοσύνης 2 περιλαμβάνουν την ακεραιότητα και την εμπιστευτικότητα των μεταδιδόμενων δεδομένων, τη μη αποποίηση παραλαβής ενός αιτήματος του πολίτη από τον πάροχο της ηλεκτρονικής υπηρεσίας, τη μη αποποίηση αποστολής των απαντήσεων, από αρμόδιο υπάλληλο που διεκπεραίωσε το σχετικό αίτημα, προς τον πολίτη, καθώς και (σε ορισμένες περιπτώσεις) τη μη αποποίηση αποστολής αιτήσεων ή/και παραλαβής απαντήσεων της διοίκησης, από τον πολίτη, την αυθεντικότητα και τη διαθεσιμότητα της υπηρεσίας και την αυθεντικοποίηση του τελικού χρήστη.

5.2.5 Επίπεδο Εμπιστοσύνης 3

Στο Επίπεδο Εμπιστοσύνης 3 εντάσσονται υπηρεσίες που απαιτούν ανταλλαγή είτε ευαίσθητων προσωπικών δεδομένων (όπως για παράδειγμα στοιχεία που αφορούν το ποινικό μητρώο ενός χρήστη) είτε υπηρεσίες ηλεκτρονικής ολοκλήρωσης επιπέδου 4, όπου ο χρήστης πραγματοποιεί ηλεκτρονικά και οικονομικές συναλλαγές. Οι επιπτώσεις που ενδέχεται να προκληθούν από κάποιο περιστατικό ασφάλειας είναι ιδιαίτερα σημαντικές, καθώς εμπλέκονται ευαίσθητα ή οικονομικά δεδομένα και ως εκ τούτου καθίσταται απαραίτητο να διασφαλιστεί υψηλός βαθμός εμπιστοσύνης για την ηλεκτρονική ταυτότητα ενός χρήστη. Οι απαιτήσεις ασφάλειας του συγκεκριμένου επιπέδου περιλαμβάνουν την ακεραιότητα και την εμπιστευτικότητα των μμεταδιδόμενων δεδομένων, τη μη αποποίηση παραλαβής ενός αιτήματος του πολίτη από τη διοίκηση, τη μη αποποίηση αποστολής των απαντήσεων, από αρμόδιο υπάλληλο, που διεκπεραίωσε το σχετικό αίτημα, προς τον πολίτη, καθώς και (σε ορισμένες περιπτώσεις) τη μη αποποίηση αποστολής αιτήσεων ή/και παραλαβής απαντήσεων της διοίκησης, από τον πολίτη, την αυθεντικότητα και τη διαθεσιμότητα της υπηρεσίας και την αυθεντικοποίηση του χρήστη.

5.3 Θεσμικό – Κανονιστικό Πλαίσιο Ψηφιακής Αυθεντικοποίησης

Η εγγραφή, ταυτοποίηση και αυθεντικοποίηση των χρηστών προϋποθέτει τη συλλογή και διαχείριση δεδομένων που αναφέρονται στην ταυτότητα των χρηστών. Εφόσον πρόκειται για εγγραφή, ταυτοποίηση και αυθεντικοποίηση νομικών προσώπων που συναλλάσσονται ηλεκτρονικά με τη Δημόσια Διοίκηση, εφαρμόζονται οι κανόνες που αφορούν την επωνυμία και τη νόμιμη εκπροσώπηση των νομικών προσώπων. Η εφαρμογή των κανόνων αυτών είναι κρίσιμη, κυρίως κατά το στάδιο της εγγραφής και του προσδιορισμού και εξέτασης της νομιμοποίησης των φυσικών προσώπων που νομιμοποιούνται να συναλλάσσονται με τη διοίκηση, δεσμεύοντας το νομικό πρόσωπο. Εν προκειμένω εφαρμόζονται αναλόγως οι γενικές διατάξεις που αφορούν την αντιπροσώπευση των νομικών προσώπων.

Στην περίπτωση που ο χρήστης είναι φυσικό πρόσωπο, η εγγραφή, ταυτοποίηση και αυθεντικοποίηση προϋποθέτουν και ταυτόχρονα συνεπάγονται περαιτέρω συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα, δηλαδή πληροφοριών που αναφέρονται σε φυσικά πρόσωπα. Η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα ρυθμίζεται από το Ν. 2472/97, οι ρυθμίσεις του οποίου αφορούν χωρίς διάκριση και την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο δημόσιο τομέα.

Το κύριο ζήτημα που τίθεται και εξετάζεται αφορά ειδικότερα τη νομική βάση της επεξεργασίας, την εφαρμογή των γενικών αρχών επεξεργασίας, τις τυχόν διαδικαστικές προϋποθέσεις νομιμότητας της επεξεργασίας, καθώς και τα δικαιώματα των προσώπων στο είδος και την έκταση των δεδομένων προσωπικού χαρακτήρα που επιτρέπεται να υφίστανται επεξεργασία για τις υπό εξέταση διαδικασίες. Αξίζει να σημειωθεί ότι, όπως προκύπτει και από τις αναφορές στον ορισμό και την έννοια των δεδομένων προσωπικού χαρακτήρα, η νομοθεσία για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, βρίσκει εφαρμογή αποκλειστικά στην επεξεργασία δεδομένων φυσικών προσώπων.

Ως προς τη νόμιμη βάση της επεξεργασίας προκαταρκτικά επισημαίνεται ότι με βάση το συνταγματικό και νομικό πλαίσιο, η επεξεργασία προσωπικών δεδομένων καταρχήν απαγορεύεται και επιτρέπεται κατ' εξαίρεση μόνο εφόσον συντρέχουν οι βάσεις νομιμότητας της επεξεργασίας που ορίζονται στα άρθρα 5-8 του ν. 2472/97. Τόσο οι ουσιαστικές όσο και οι διαδικαστικές προϋποθέσεις νομιμότητας της επεξεργασίας διαφοροποιούνται καταρχήν με κριτήριο το είδος και την κατηγορία των δεδομένων («απλά» και ευαίσθητα και ειδικότερες κατηγορίες ευαίσθητων δεδομένων) ενώ ο νόμος περιέχει ειδικές ρυθμίσεις για τη «διασύνδεση» ως μορφή επεξεργασίας δεδομένων.

5.3.1 Νομική Βάση Επεξεργασίας

Στο βαθμό που αναφερόμαστε στις διαδικασίες Εγγραφής, Αυθεντικοποίησης και Ταυτοποίησης φυσικών προσώπων και συγκεκριμένων συναλλασσομένων με τη Δημόσια Διοίκηση, οι νόμιμες βάσεις επεξεργασίας μπορεί να συνίστανται διαζευκτικά: α) στη συγκατάθεση του προσώπου, β) στην εκπλήρωση νόμιμης υποχρέωσης του υπεύθυνου επεξεργασίας και γ) στην εκπλήρωση έργου δημοσίου συμφέροντος ή στην άσκηση δημόσιας εξουσίας.

Στη συγκεκριμένη περίπτωση, η συγκατάθεση του προσώπου τίθεται στο άρθρο 5 παρ. 1 του ν. 2472/97 ως κανόνας για τη σύννομη επεξεργασία προσωπικών δεδομένων, προβλέπονται ωστόσο εξαιρέσεις στην παράγραφο 2. Μία από αυτές τις εξαιρέσεις προβλέπει τα ακόλουθα: "*Κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς τη συγκατάθεση, όταν: β) Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο*".

Από τους συντάκτες του παρόντος παραδοτέου κειμένου για το ΠΨΑ δεν προτείνεται η εισαγωγή ειδικής νομοθετικής ρύθμισης, καθώς το γενικό πνεύμα της νομοθεσίας και η σχετική συνταγματική ρύθμιση προτάσσει τη συγκατάθεση ως εκδήλωση του δικαιώματος προστασίας

προσωπικών δεδομένων. Εξάλλου, στο βαθμό που η χρήση υπηρεσιών ηλεκτρονικής διακυβέρνησης δεν είναι υποχρεωτική για τους πολίτες, η παροχή συγκατάθεσης είναι ένας τρόπος για να γνωρίζουν οι πολίτες τις συνέπειες της ηλεκτρονικής αίτησης και παροχής υπηρεσιών. Υπενθυμίζεται ότι η συγκατάθεση, σύμφωνα με την οικεία νομοθεσία (άρθρο 2 ι του ν. 2472/97), είναι ρητή, ειδική και «κατόπιν πληροφόρησης». Δεν προτείνεται συνεπώς ουδεμία απόκλιση από τον κανόνα της συγκατάθεσης.

Ο ν. 2472/97 προκρίνει τη συγκατάθεση του προσώπου ως κανόνα. Κατ' εξαίρεση ή ελλείψει αυτής της συγκατάθεσης ισχύουν οι άλλες, προαναφερόμενες νόμιμες βάσεις επεξεργασίας. Εφόσον νομοθετική διάταξη, ειδική και μεταγενέστερη του ν. 2472/97, προβλέπει την εγγραφή/ ταυτοποίηση/ αυθεντικοποίηση ως υποχρέωση των συναλλασσομένων και αντίστοιχα ως αρμοδιότητα της Δημόσιας Διοίκησης τότε ενδέχεται να μην απαιτείται η ύπαρξη συναίνεσης του προσώπου, στο βαθμό που από το σύνολο της ρύθμισης δεν τίθεται θέμα προσβολής του συνταγματικού δικαιώματος προστασίας των προσωπικών δεδομένων (άρθρο 9Α του Συντάγματος).

Η συγκατάθεση σύμφωνα με το ν. 2472/97, όπως ισχύει, πρέπει να είναι ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή, και με πλήρη επίγνωση, και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Η ενημέρωση αυτή περιλαμβάνει πληροφόρηση τουλάχιστον για το σκοπό της επεξεργασίας, τα δεδομένα ή τις κατηγορίες δεδομένων που αφορά η επεξεργασία, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, καθώς και το όνομα, την επωνυμία και τη διεύθυνση του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου του. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα.

Η συγκατάθεση προσδιορίζεται από το νόμο ως ρητή, συνεπώς απορρίπτεται η εικαζόμενη ή σιωπηρή συγκατάθεση: η αίτηση για ηλεκτρονική παροχή μιας υπηρεσίας ή συναλλαγής ή η αποδοχή μιας τέτοιας υπηρεσίας ή συναλλαγής δεν επέχει θέση συγκατάθεσης, τουλάχιστον όταν πρόκειται για δηλώσεις/ υπηρεσίες/ συναλλαγές που παράγουν έννομα (CERI, 2003).

Ένα περαιτέρω ζήτημα αναφέρεται στην εγκυρότητα της «ηλεκτρονικής συγκατάθεσης»: οι διατάξεις του ν. 3471/06 που αφορούν την προστασία των προσωπικών δεδομένων στο πεδίο των ηλεκτρονικών επικοινωνιών, προβλέπουν και την παροχή συγκατάθεσης με ηλεκτρονικά μέσα. Στην περίπτωση αυτή ο νόμος απαιτεί να εξασφαλίζει ο υπεύθυνος επεξεργασίας ότι ο συνδρομητής ή χρήστης ενεργεί με πλήρη επίγνωση των συνεπειών που έχει η δήλωσή του η οποία καταγράφεται με ασφαλή τρόπο και είναι ανά πάσα στιγμή προσβάσιμη στο χρήστη ή συν-

δρομητή και μπορεί οποτεδήποτε να ανακληθεί. Το άρθρο 5 του ν. 3471/06 [που αντικατέστησε τον ν. 2774/99 (πρώτο μέρος) και τροποποίησε εν μέρει τον γενικό ν. 2472/97 για την επεξεργασία και προστασία προσωπικών δεδομένων] αφορά την προστασία απορρήτου και ιδιωτικότητας στις ηλεκτρονικές επικοινωνίες. Δεν τροποποιεί τον ορισμό της συγκατάθεσης, όπως αυτός περιλαμβάνεται στο άρθρο 2 ι του ν. 2472/97. Η τελευταία ρύθμιση μπορεί, βέβαια, να ερμηνευτεί κατά τρόπο ώστε να καταλαμβάνει και την ηλεκτρονική συγκατάθεση. Είναι όμως θέμα ερμηνείας και όχι συγκεκριμένης ρύθμισης. Ακριβώς λόγω της ειδικότητάς της αυτή η ρύθμιση, το πεδίο εφαρμογής της οποίας αφορά τα δημόσια δίκτυα επικοινωνιών, δεν είναι δυνατόν να χρησιμεύσει αυτοτελώς για τη θεμελίωση της δυνατότητας της ηλεκτρονικής συγκατάθεσης.

Όπως προκύπτει από την 18.07.2007 γνωμοδότηση (48/07) της Αρχής Προστασίας Προσωπικών Δεδομένων, η Αρχή αποδέχεται ως νομική βάση της επεξεργασίας την ελεύθερη, ρητή και ειδική συγκατάθεση των υποκειμένων των δεδομένων όπως την ορίζει ο ν. 2472/1997 σε συνδυασμό και με το ν. 3471/2006 για την προστασία των προσωπικών δεδομένων, στις ηλεκτρονικές επικοινωνίες.

Εάν πρόκειται για την επεξεργασία ευαίσθητων δεδομένων, η συγκατάθεση πρέπει αναγκαστικά να περιλαμβάνει έγγραφο τύπο. Η ειδικότερη διαμόρφωση της διαδικασίας για την παροχή συγκατάθεσης, εξαρτάται από το μοντέλο παροχής ηλεκτρονικής υπηρεσίας που θα επιλεγεί. Το ενδεχόμενο να παρέχεται μία γενική συγκατάθεση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, προσκρούει στην απαίτηση της «ειδικής δήλωσης βούλησης», ώστε να είναι έγκυρη η συγκατάθεση. Οπωσδήποτε και σε κάθε περίπτωση όπου απαιτείται έγγραφη συγκατάθεση, όπως στην περίπτωση της επεξεργασίας ευαίσθητων δεδομένων, η ηλεκτρονική παροχή της μπορεί να γίνει δεκτή - με βάση τις γενικές διατάξεις - μόνον εφόσον πρόκειται για «προηγμένη ηλεκτρονική υπογραφή» (άρθρο 3 Π.Δ. 150/2001).

5.3.2 Εφαρμογή Γενικών Αρχών Επεξεργασίας

Οι γενικές αρχές επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως κατοχυρώνονται στο άρθρο 4 του ν. 2472/97 και έχουν ερμηνευτεί από την Αρχή Προστασίας Προσωπικών Δεδομένων, ισχύουν και στον προσδιορισμό των όρων επεξεργασίας, στο πλαίσιο των διαδικασιών αυθεντικοποίησης και ταυτοποίησης.

Συγκεκριμένα η επεξεργασία πρέπει να συνάδει προς τις αρχές της αναλογικότητας και του σκοπού. Από την αρχή της αναλογικότητας απορρέει καταρχήν η αρχή της φειδούς ως προς την επεξεργασία δεδομένων: θα πρέπει να συλλέγονται τα ελάχιστα απαιτούμενα προσωπικά δε-

δομένα για την εκπλήρωση του σκοπού, δηλαδή της παροχής συγκεκριμένης υπηρεσίας ή κατηγορίας υπηρεσιών. Θα πρέπει να συλλέγονται εκείνα και μόνο όσα είναι αναγκαία και κατάλληλα για την εκπλήρωση του σκοπού αυτού (αναγκαιότητα, προσφορότητα, υπό στενή έννοια αναλογικότητα των δεδομένων). Όσον αφορά την αρχή του σκοπού, αυτή επιτάσσει να μη χρησιμοποιούνται τα δεδομένα για σκοπούς μη συμβατούς με αυτούς για τους οποίους έχουν συλλεχθεί (Μήτρου, 2006).

Οι αρχές αυτές ισχύουν για την ταυτοποίηση και τα διάφορα στάδια αυτής. Είναι προφανές ότι το είδος της υπηρεσίας που προσφέρεται, και το αντίστοιχο επίπεδο εμπιστοσύνης προσδιορίζει και εάν και ποια προσωπικά δεδομένα πρέπει να συλλέγονται και να υπόκεινται σε επεξεργασία. Εξ αυτού απορρέουν ειδικότερα οι ακόλουθες αρχές:

- Στην περίπτωση υπηρεσιών (πληροφόρησης και αναζήτησης προτύπων και φορμών κλπ.) για τις οποίες δεν είναι αναγκαίος ο προσδιορισμός της ταυτότητας του συναλλασσόμενου, αυτές θα πρέπει να προσφέρονται χωρίς να λαμβάνει χώρα καμία συλλογή δεδομένων προσωπικού χαρακτήρα.
- Στην περίπτωση υπηρεσιών πληροφόρησης, αυτές μπορούν να παρέχονται χωρίς να είναι αναγκαία η καταχώριση του συνόλου της IP διεύθυνσης του αποδέκτη της υπηρεσίας, εφόσον δεν είναι αναγκαίο για την παροχή της υπηρεσίας ή την τυχόν χρέωσή της.
- Στην περίπτωση απλών υπηρεσιών (π.χ. Newsletter), αυτές μπορούν να παρέχονται με αναγκαία μόνη την καταχώριση της ηλεκτρονικής διεύθυνσης του παραλήπτη χωρίς να είναι αναγκαία η συλλογή και επεξεργασία ονοματεπώνυμου και ταχυδρομικής διεύθυνσης.

Η αυθεντικοποίηση και η ταυτοποίηση του συναλλασσόμενου θα πρέπει να παραλείπεται, εφόσον αυτή δεν απαιτείται εν γένει από το νόμο για την παροχή της ίδιας υπηρεσίας off-line (υπό την ουσιαστική έννοια της νομικά δεσμευτικής ρύθμισης, δηλ. μπορεί να πρόκειται και για υπουργική απόφαση που εκδίδεται κατ' εξουσιοδότηση νόμου). Αντίθετα, εάν στην «κλασική» παροχή της υπηρεσίας είναι αναγκαία η ταυτοποίηση, κατά μείζονα λόγο πρέπει αυτή να απαιτείται στο πλαίσιο της ηλεκτρονικής διεκπεραίωσης. Μία παράμετρος που καθιστά αναγκαία τη μονοσήμαντη ταυτοποίηση του συναλλασσόμενου είναι η πρόσβαση σε προσωπικά δεδομένα αυτού, ανεξαρτήτως εάν πρόκειται για "απλά" ή ευαίσθητα, προκειμένου να καταστεί δυνατή η παροχή της υπηρεσίας.

Στην περίπτωση υπηρεσιών για την παροχή των οποίων κρίνεται αναγκαία η αυθεντικοποίηση και ταυτοποίηση του χρήστη – λήπτη μιας υπηρεσίας, τα δεδομένα που συλλέγονται, θα πρέπει να περιορίζονται στα αναγκαία για την ταυτοποίηση που απαιτούνται για την παροχή της συγκεκριμένης υπηρεσίας. Εφόσον ζητούνται περαιτέρω μη αναγκαία στοιχεία, θα πρέπει να επισημαίνεται στο συναλλασσόμενο με τη διοίκηση η μη υποχρεωτικότητα της παροχής των συγκεκριμένων στοιχείων.

Από τις ίδιες αρχές απορρέει η αναγκαιότητα τεχνικού και οργανωτικού διαχωρισμού των δεδομένων που είναι απαραίτητα για την ταυτοποίηση και αυθεντικοποίηση του συναλλασσόμενου με τη διοίκηση και των δεδομένων που αφορούν στο περιεχόμενο της αιτηθείσας ή παρεχόμενης πληροφορίας και υπηρεσίας, καθώς ενδέχεται να μην ταυτίζονται οι χειριστές των δύο σταδίων.

Στοιχείο της ποιότητας των δεδομένων, στενά συνδεδεμένο και με την αρχή της αναλογικότητας, είναι η επιταγή για ακρίβεια των δεδομένων. Τα προσωπικά δεδομένα πρέπει να είναι αληθή, ακριβή και συνεπώς να υπόκεινται σε επικαιροποίηση, ώστε να εξακολουθούν να ανταποκρίνονται στην πραγματικότητα. Η ανακρίβεια, η διατήρηση αναληθών ή μη επικαιροποιημένων δεδομένων ενδέχεται να εκθέσει τα άτομα σε ιδιαίτερους κινδύνους και διακρίσεις.

Σύμφωνα με το άρθρο 4 δ του Ν. 2472/97 τα δεδομένα πρέπει να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους. Η κρίση για την εκπλήρωση του σκοπού και την καταστροφή των δεδομένων δεν επαφίεται στον υπεύθυνο επεξεργασίας, αλλά ελέγχεται από την Αρχή Προστασίας Προσωπικών Δεδομένων. Μετά την παρέλευση της περιόδου αυτής, η Αρχή μπορεί, με αιτιολογημένη απόφασή της, να επιτρέπει τη διατήρηση δεδομένων προσωπικού χαρακτήρα για ιστορικούς επιστημονικούς ή στατιστικούς σκοπούς, εφ΄ όσον κρίνει ότι δεν θίγονται σε κάθε συγκεκριμένη περίπτωση τα δικαιώματα των υποκειμένων τους ή και τρίτων.

Σύμφωνα με τη δεύτερη παράγραφο του άρθρου 4 του ν. 2472/97, όπως τροποποιήθηκε ως άνω σύμφωνα με το άρθρο 20 παρ. 2 Ν. 3471/2006, η τήρηση των διατάξεων της προηγούμενης παραγράφου βαρύνει τον υπεύθυνο επεξεργασίας. Δεδομένα προσωπικού χαρακτήρα που έχουν συλλεχθεί ή υφίστανται επεξεργασία κατά παράβαση της προηγούμενης παραγράφου καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας. Η Αρχή, εάν εξακριβώσει αυτεπαγγέλτως ή μετά από σχετική καταγγελία παράβαση των διατάξεων της προηγούμενης παραγράφου, επι-

βάλλει τη διακοπή της συλλογής ή της επεξεργασίας και την καταστροφή των δεδομένων προσωπικού χαρακτήρα που έχουν ήδη συλλεγεί ή τύχει επεξεργασίας.

5.3.3 Τα Δικαιώματα των Προσώπων

Η νομοθεσία για την προστασία προσωπικών δεδομένων (ν. 2427/97) περιέχει ειδικούς κανόνες για τα δικαιώματα των προσώπων (άρθρα 11-14). Ανεξάρτητα από τη νόμιμη βάση της συλλογής και επεξεργασίας δεδομένων (για ταυτοποίηση κλπ.) είναι αναγκαία η ενημέρωση των προσώπων για τη συλλογή και παραγωγή δεδομένων που συνεπάγονται οι διαδικασίες της ταυτοποίησης και αυθεντικοποίησης. Ο υπεύθυνος επεξεργασίας οφείλει (άρθρο 11), κατά το στάδιο της συλλογής των σχετικών δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με τρόπο πρόσφορο και σαφή το συναλλασσόμενο-αιτούντα, που είναι το υποκείμενο των δεδομένων, για τα εξής τουλάχιστον στοιχεία:

- την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του,
- το σκοπό της επεξεργασίας,
- τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων,
- την ύπαρξη του δικαιώματος πρόσβασης.

Είναι επίσης, όπως προαναφέρθηκε, αναγκαίο να ενημερώνεται ο συναλλασσόμενος για την υποχρεωτικότητα ή μη παροχής των στοιχείων, καθώς και για τις συνέπειες μη παροχής υποχρεωτικών στοιχείων.

Ο νόμος δεν προσδιορίζει τους ειδικότερους τρόπους της ενημέρωσης. Η ενημέρωση μπορεί να γίνει και ηλεκτρονικά, είτε με γενική αναγραφή των σχετικών όρων στο δικτυακό τόπο, είτε εξειδικευμένα προς το συναλλασσόμενο με τη διοίκηση. Ακόμη και εάν επιλέγεται η πρώτη εναλλακτική λύση, σε κάθε περίπτωση είναι σκόπιμο να επισημαίνεται στον ηλεκτρονικά συναλλασσόμενο ειδικά και συγκεκριμένα η ύπαρξη και ο «τόπος» της ενημέρωσης.

Κατ' εφαρμογή των γενικών κανόνων, το υποκείμενο των δεδομένων (*Data Subject*), εν προκειμένω ο συναλλασσόμενος με τη Δημόσια Διοίκηση, έχει τα δικαιώματα της πρόσβασης, διόρθωσης και αντίρρησης ως προς τα δεδομένα που τον αφορούν, όπως αυτά προσδιορίζονται στα άρθρα 12 και 13 του Ν. 2472/97, όπως ισχύει.

5.3.4 Συμμόρφωση με Διαδικαστικές Προϋποθέσεις

Ο Ν. 2472/97 έχει εισαγάγει σύστημα γνωστοποίησης των αρχείων και επεξεργασίας δεδομένων προσωπικού χαρακτήρα (άρθρο 6). Η συλλογή και επεξεργασία δεδομένων αναγκαίων για την ταυτοποίηση και την αυθεντικοποίηση, θα πρέπει να γνωστοποιείται στην Αρχή Προστασίας Προσωπικών Δεδομένων.

Με τη γνωστοποίηση, ο υπεύθυνος επεξεργασίας πρέπει απαραιτήτως να δηλώνει:

- Το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο του και τη διεύθυνσή του.
- Τη διεύθυνση όπου είναι εγκατεστημένο το αρχείο ή ο κύριος εξοπλισμός που υποστηρίζει την επεξεργασία.
- Την περιγραφή του σκοπού της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που περιέχονται ή πρόκειται να περιληφθούν στο αρχείο.
- Το είδος των δεδομένων προσωπικού χαρακτήρα που υφίστανται ή πρόκειται να υποστούν επεξεργασία ή περιέχονται ή πρόκειται να περιληφθούν στο αρχείο.
- Το χρονικό διάστημα για το οποίο προτίθεται να εκτελεί την επεξεργασία ή να διατηρήσει το αρχείο.
- Τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους ανακοινώνει ή ενδέχεται να ανακοινώνει, τα δεδομένα προσωπικού χαρακτήρα.
- Τις ενδεχόμενες διαβιβάσεις και το σκοπό της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες.
- Τα βασικά χαρακτηριστικά του συστήματος και των μέτρων ασφαλείας του αρχείου ή της επεξεργασίας.

Η γνωστοποίηση της συλλογής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της ταυτοποίησης και αυθεντικοποίησης, μπορεί να αποτελούν και μέρος γενικότερης γνωστοποίησης της συλλογής και επεξεργασίας προσωπικών δεδομένων για την παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης.

Στην περίπτωση που είναι γνωστό ή πιθανολογείται ότι θα λάβει χώρα συλλογή και επεξεργασία «ευαίσθητων δεδομένων», όπως ορίζονται στο ν. 2472/97, τότε είναι αναγκαία η προηγούμενη γνωστοποίηση και η αίτηση προς την Αρχή Προστασίας Προσωπικών Δεδομένων για παροχή σχετικής άδειας (άρθρο 7 ν. 2472/97).

Στη διαδικασία της προηγούμενης γνωστοποίησης / άδειας υπόκειται και η διασύνδεση αρχείων (όπως ορίζεται στο άρθρο 2 στ του ν. 2472/97, δηλ. στη δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με δεδομένα άλλου αρχείου ή αρχείων). Συγκεκριμένα, εάν για την ταυτοποίηση και αυθεντικοποίηση πρόκειται να γίνει διασύνδεση, απαιτείται προηγούμενη άδεια της Αρχής («άδεια διασύνδεσης»), εάν α) ένα τουλάχιστον από τα αρχεία που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα, β) με τη διασύνδεση πρόκειται να αποκαλυφθούν ευαίσθητα δεδομένα ή γ) εάν για την πραγματοποίηση της διασύνδεσης πρόκειται να γίνει χρήση ίδιου (ενιαίου) κωδικού αριθμού. Η άδεια διασύνδεσης της προηγούμενης παραγράφου χορηγείται ύστερα από ακρόαση των υπεύθυνων επεξεργασίας των αρχείων και αναφέρει απαραιτήτως το σκοπό για τον οποίο η διασύνδεση θεωρείται αναγκαία, το είδος των δεδομένων προσωπικού χαρακτήρα που αφορά η διασύνδεση, το χρονικό διάστημα για το οποίο επιτρέπεται η διασύνδεση, καθώς και τυχόν όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία των δικαιωμάτων και ελευθεριών και ιδίως του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων.

Εν γένει διαφαίνεται ότι το κανονιστικό πλαίσιο που αφορά την επεξεργασία προσωπικών δεδομένων, όπως αυτή περιγράφεται παραπάνω, είναι επαρκές. Τυχόν ειδικά ζητήματα μπορούν να αντιμετωπιστούν με την εξειδίκευση γενικών κανόνων κατά την εφαρμογή της νομοθεσίας και κυρίως κατά την εφαρμογή των αρχών της αναλογικότητας και του σκοπού. Τα όρια της νόμιμης δράσης συμπροσδιορίζονται εξάλλου και από τυχόν όρους και προϋποθέσεις που θα θέσει η Αρχή Προστασίας Προσωπικών Δεδομένων, αποφαινόμενη επί των αιτήσεων για άδειες επεξεργασίας ευαίσθητων δεδομένων και άδειες διασύνδεσης.

5.3.5 Υποχρεώσεις της Δημόσιας Διοίκησης

Οι ενέργειες που θα πρέπει να εκτελέσει η Διοίκηση σχετικά με την αυθεντικοποίηση πολιτών, επιχειρήσεων και φορέων σε υπηρεσίες ηλεκτρονικής διακυβέρνησης περιλαμβάνουν τα εξής:

- Θα πρέπει να συνταχθούν έντυπα για την παροχή και λήψη συγκατάθεσης, τα οποία θα δίδονται στους αιτούμενους την εγγραφή. Αξίζει να σημειωθεί, ότι ο Ν. 2472/97 απαιτεί έγγραφο μόνο για την επεξεργασία ευαίσθητων δεδομένων. Ωστόσο καθώς η συγκατάθεση θα πρέπει να είναι σαφής, ρητή, ειδική και «ενημερωμένη» συνιστάται να ακολουθείται ο έγγραφος τύπος ακόμη και για την περίπτωση αυτή.

- Κατά την αίτηση για εγγραφή σε διάφορες υπηρεσίες, θα πρέπει να καθίσταται σαφές στους αιτούντες, εάν και ποια δεδομένα είναι αναγκαία για την εγγραφή.
- Κατά την αίτηση για λήψη υπηρεσιών θα πρέπει να καθίσταται σαφές στους αιτούντες ποια και τι είδους δεδομένα είναι αναγκαία για την επεξεργασία και τη διεκπεραίωση της αίτησής τους.
- Κατά την αίτηση θα πρέπει να γίνεται σαφής διαχωρισμός, τόσο στους αιτούντες όσο και στους χειριστές, μεταξύ των απαραίτητων δεδομένων και των δεδομένων των οποίων η παροχή είναι προαιρετική.
- Θα πρέπει να γίνεται διαχωρισμός των δεδομένων ταυτοποίησης και των δεδομένων που αφορούν στο περιεχόμενο της αιτηθείσας ή παρεχόμενης πληροφορίας και υπηρεσίας.
- Ανεξάρτητα από τη συγκατάθεση, δηλ. ακόμη και εάν η παροχή δεδομένων προβλέπεται ρητά από διάταξη νόμου ως υποχρεωτική (όπως π.χ. στις φορολογικές δηλώσεις), θα πρέπει, κατά την εγγραφή σε υπηρεσίες, να ενημερώνονται οι αιτούντες, σύμφωνα με το άρθρο 11 του Ν. 2472/97, τουλάχιστον για την ταυτότητά του υπεύθυνου επεξεργασίας των δεδομένων και την ταυτότητα του τυχόν εκπροσώπου του, το σκοπό της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων και την ύπαρξη του δικαιώματος πρόσβασης.
- Η ενημέρωση μπορεί να γίνει και ηλεκτρονικά, με γενική αναγραφή των σχετικών όρων στο δικτυακό τόπο. Στην περίπτωση αυτή θα πρέπει ο «τόπος» της ενημέρωσης να είναι εμφανής και να επισημαίνεται στον εγγραφόμενο - ηλεκτρονικά συναλλασσόμενο.
- Θα πρέπει να γίνουν όλες οι απαραίτητες διαδικαστικές ενέργειες έναντι της Αρχής Προστασίας Προσωπικών Δεδομένων που απαιτούνται κατά περίπτωση από το νόμο: α) γνωστοποίηση για τη συλλογή και επεξεργασία απλών δεδομένων (συμπεριλαμβάνονται τα οικονομικά δεδομένα, αυτά δηλ. που καλύπτονται από το φορολογικό απόρρητο), β) αίτηση για άδεια στην περίπτωση της επεξεργασίας ευαίσθητων δεδομένων γ) αίτηση για άδεια διασύνδεσης εφόσον γίνεται διασύνδεση αρχείων, εκ των οποίων έστω το ένα περιλαμβάνει ευαίσθητα ή γίνεται χρήση ενιαίου κωδικού αριθμού. Οι ενέργειες αυτές είναι απαραίτητες εφόσον η παροχή υπηρεσιών δεν καλύπτεται από προηγούμενες γνωστοποιήσεις/ αιτήσεις προς την Αρχή. Στην περίπτωση αυτή, δηλαδή όταν έχουν κατα-

τεθεί γνωστοποιήσεις/ αιτήσεις που δεν καλύπτουν την ταυτοποίηση/ ηλεκτρονική παροχή υπηρεσιών, πρέπει να κατατεθούν συμπληρωματικές γνωστοποιήσεις/ αιτήσεις ή τροποποίηση των κατατεθειμένων σύμφωνα με το άρθρο 6 § 4 του Ν. 2472/97.

- Θα πρέπει να επισημαίνεται στους χειριστές των αιτήσεων εγγραφής ή των αιτήσεων για ηλεκτρονική παροχή υπηρεσιών ότι τα προσωπικά δεδομένα θα πρέπει να είναι ακριβή και επικαιροποιημένα. Θα ήταν ίσως σκόπιμο να εισαχθούν συγκεκριμένες προθεσμίες (π.χ. ανά έτος) στο πλαίσιο των οποίων θα ελέγχεται η επικαιροποίηση των δεδομένων.
- Θα πρέπει να επισημαίνεται στους χειριστές των αιτήσεων εγγραφής ή των αιτήσεων για ηλεκτρονική παροχή υπηρεσιών η υποχρέωση διαγραφής/ καταστροφής δεδομένων που δεν είναι πλέον αναγκαία για την εκπλήρωση ενός σκοπού. Λόγω της πολλαπλότητας των σκοπών δεν είναι δυνατόν να γίνει περαιτέρω εξειδίκευση της συγκεκριμένης υποχρέωσης.
- Τα αρχεία-δεδομένα θα πρέπει να καταστρέφονται μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού. Για την καταστροφή θα πρέπει να ακολουθούνται οι οδηγίες της Αρχής Προστασίας Προσωπικών Δεδομένων που περιέχονται στη σχετική Οδηγία 1/2005[4].

5.4 Ταυτοποίηση κατά τη Χρήση Ηλεκτρονικών Υπηρεσιών

Με τον όρο ταυτοποίηση, υπό το πρίσμα του ΠΨΑ, νοείται η διαδικασία δήλωσης ταυτότητας από το χρήστη στις υπηρεσίες ηλεκτρονικής διακυβέρνησης. Καθώς οι χρήστες-πολίτες αξιοποιούν διαφορετικού είδους «ταυτότητες» στις συναλλαγές τους με τη Δημόσια Διοίκηση, η διαδικασία-μέθοδος ταυτοποίησης που θα αξιοποιηθεί στις αντίστοιχες υπηρεσίες ηλεκτρονικής διακυβέρνησης, θα επηρεάσει σε μεγάλο βαθμό το ΠΨΑ, καθώς οι διαφορετικοί τρόποι και μέθοδοι ταυτοποίησης δημιουργούν διαφορετικού είδους νομικούς, θεσμικούς ή ακόμα και «τεχνικούς» περιορισμούς.

Λαμβάνοντας υπόψη την Ελληνική συνταγματική και έννομη τάξη και τις υπάρχουσες μεθόδους ταυτοποίησης για συναλλαγές με το Ελληνικό Δημόσιο, προτείνεται η ταυτοποίηση των

[4] Οδηγίες Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: http://www.dpa.gr/portal/page?_pageid=33,120908&_dad=portal&_schema=PORTAL

χρηστών σε ηλεκτρονικές υπηρεσίες της δημόσιας διοίκησης μέσω της Κεντρικής Διαδικτυακής Πύλης (ΚΔΠ), με αξιοποίηση ξεχωριστών αναγνωριστικών των χρηστών ανά υπηρεσία.

Με τη συγκεκριμένη προτεινόμενη τεχνική ταυτοποίησης, με χρήση διαφορετικού αναγνωριστικού για κάθε υπηρεσία, οι διαδικασίες της εγγραφής και της αυθεντικοποίησης πραγματοποιούνται στην ΚΔΠ, χωρίς να απαιτείται να έχουν οι χρήστες προηγουμένως εγγραφεί στις ανεξάρτητες ηλεκτρονικές υπηρεσίες, αλλά και ενδεχόμενη εγγραφή τους σε αυτές να μη σχετίζεται με τη διαδικασία αυθεντικοποίησης στην ΚΔΠ και να μην προκύπτει καμία απολύτως συσχέτιση ή πρόβλημα από το γεγονός αυτό για την ολοκλήρωση των παρεχόμενων υπηρεσιών. Κατά τη διάρκεια της εγγραφής του χρήστη στην ΚΔΠ, ο χρήστης πρέπει να εισάγει τα διαφορετικά αναγνωριστικά που απαιτεί ο κάθε φορέας προκειμένου να τον ταυτοποιήσει. Τα αναγνωριστικά αυτά (π.χ. ΑΦΜ, ΑΔΤ, ΑΜΚΑ κλπ.), αν επιθυμεί ο χρήστης, είναι δυνατόν να αποθηκεύονται στην ΚΔΠ και να συνθέτουν τον ψηφιακό φάκελο αναγνωριστικών για το συγκεκριμένο χρήστη. Όταν ο χρήστης επιθυμεί να χρησιμοποιήσει μία ηλεκτρονική υπηρεσία, η ΚΔΠ αναζητά στον ψηφιακό φάκελο αναγνωριστικών του χρήστη, το αναγνωριστικό που απαιτείται για την ταυτοποίησή του στη συγκεκριμένη υπηρεσία. Εάν η αναζήτηση είναι επιτυχής, το αναγνωριστικό αποστέλλεται στον εξυπηρετητή της αντίστοιχης υπηρεσίας, προκειμένου ο χρήστης να ταυτοποιηθεί και να ξεκινήσει η διαδικασία της αυθεντικοποίησής του. Σε περίπτωση που η αναζήτηση δεν είναι επιτυχής, ο χρήστης ενημερώνεται από την ΚΔΠ ότι δεν μπορεί να χρησιμοποιήσει τη συγκεκριμένη ηλεκτρονική υπηρεσία.

5.5 Επίπεδα Αυθεντικοποίησης

Με τον όρο "αυθεντικοποίηση" ορίζεται η διαδικασία πιστοποίησης και επιβεβαίωσης της ταυτότητας των χρηστών, η οποία σε κάθε περίπτωση βασίζεται στα διαπιστευτήρια που κατέχει ο χρήστης. Είναι συνεπές με τα όσα έχουν αναφερθεί προηγουμένως ότι στις υπηρεσίες ηλεκτρονικής διακυβέρνησης θα πρέπει να υποστηρίζονται εναλλακτικοί τρόποι αυθεντικοποίησης, με βάση τη βεβαιότητα που απαιτείται για την ορθότητα της ψηφιακής ταυτότητας μιας οντότητας. Με άλλα λόγια όσο υψηλότερο είναι το επίπεδο εμπιστοσύνης στο οποίο εντάσσεται μία υπηρεσία, τόσο ισχυρότερος μηχανισμός αυθεντικοποίησης απαιτείται. Επιπλέον θα πρέπει να παρέχεται στους χρήστες η δυνατότητα πρόσβασης σε υπηρεσίες χαμηλότερου επιπέδου, όταν αυθεντικοποιούνται με την αξιοποίηση ισχυρότερων διακριτικών, σε σχέση με αυτό που απαιτεί η υπηρεσία, με βάση το επίπεδο εμπιστοσύνης που εντάσσεται. Με αυτή τη λογική, το

ΠΨΑ ορίζει τρία (3) Επίπεδα Αυθεντικοποίησης που κατηγοριοποιούν τους μηχανισμούς και τα διακριτικά αυθεντικοποίησης ανάλογα με την ισχύ τους.

5.5.1 Επίπεδο Αυθετικοποίησης 0

Στο συγκεκριμένο επίπεδο δεν απαιτείται αυθεντικοποίηση του χρήστη, καθώς οποιαδήποτε οντότητα δύναται να έχει πρόσβαση στις πληροφορίες που θεωρούνται δημόσιες. Συνήθως, τέτοιου τύπου υπηρεσίες είναι όσες παρέχουν πληροφοριακό υλικό. Σε αυτό το επίπεδο αυθεντικοποίησης θα πρέπει να διασφαλίζονται, κατ' ελάχιστον, οι ακόλουθες απαιτήσεις ασφάλειας:

- Ακεραιότητα του παρεχόμενου πληροφοριακού υλικού
- Αυθεντικότητα Υπηρεσίας

Το Επίπεδο Αυθεντικοποίησης 0 σχετίζεται με το επίπεδο εμπιστοσύνης 0, καθώς δεν απαιτείται επιβεβαίωση της ορθότητας της ψηφιακής ταυτότητας του τελικού χρήστη. Τέλος, για την αξιοποίηση υπηρεσιών που εντάσσονται στο επίπεδο αυθεντικοποποίησης 0, δεν απαιτείται κάποιος μηχανισμός αυθεντικοποίησης.

5.5.2 Επίπεδο Αυθεντικοποίησης 1

Στο Επίπεδο Αυθεντικοποίησης 1 απαιτείται μικρή έως μέτρια βεβαιότητα για την ορθότητα της ψηφιακής ταυτότητας μιας οντότητας, καθώς αφορούν υπηρεσίες στις οποίες δικαίωμα πρόσβασης έχουν μόνο εξουσιοδοτημένες οντότητες. Τέτοιου είδους υπηρεσίες θεωρούνται αυτές που υποστηρίζουν τη δυνατότητα παροχής αιτήσεων στους χρήστες για περαιτέρω (*Off-Line*) επεξεργασία και την πραγματοποίηση της συναλλαγής με το φορέα σε φυσικό επίπεδο.

Το Επίπεδο Αυθεντικοποίησης 1 σχετίζεται με τα επίπεδα εμπιστοσύνης 1 και 2, καθώς απαιτείται έως και μέτρια βεβαιότητα για την ορθότητα της ψηφιακής ταυτότητας του χρήστη. Σε αυτό το επίπεδο αυθεντικοποίησης θα πρέπει να διασφαλίζονται, κατ' ελάχιστον, οι ακόλουθες απαιτήσεις ασφάλειας :

- Εμπιστευτικότητα των
    - δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη (τήρηση κανόνων προστασίας προσωπικών δεδομένων)
    - διαπιστευτηρίων του χρήστη
- Ακεραιότητα των

- δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη
- διαπιστευτηρίων του χρήστη
- δεδομένων που λαμβάνονται από την ηλεκτρονική υπηρεσία

- Αυθεντικότητα υπηρεσίας

Τέλος, για την αξιοποίηση υπηρεσιών που εντάσσονται στο επίπεδο αυθεντικοποίησης 1, προτείνεται η χρήση των εξής μηχανισμών αυθεντικοποίησης:

- Συνθηματικά (*Passwords*) και
- Συνθηματικά μιας χρήσης (*One-time Passwords*).

5.5.3 Επίπεδο Αυθεντικοποίησης 2

Στο Επίπεδο Αυθεντικοποίησης 2 απαιτείται υψηλή βεβαιότητα για την ορθότητα της ψηφιακής ταυτότητας μιας οντότητας, καθώς είναι εξαιρετικά κρίσιμο να εξασφαλιστεί ότι μόνο εξουσιοδοτημένα πρόσωπα έχουν τη δυνατότητα πρόσβασης στις προσφερόμενες υπηρεσίες. Εδώ εντάσσονται οι ηλεκτρονικές υπηρεσίες που επεξεργάζονται ευαίσθητα προσωπικά δεδομένα ή υποστηρίζουν τη διενέργεια οικονομικών συναλλαγών. Το επίπεδο αυθεντικοποίησης 2 σχετίζεται με το επίπεδο εμπιστοσύνης 3, καθώς απαιτείται υψηλή βεβαιότητα για την ορθότητα της ψηφιακής ταυτότητας του χρήστη. Ο μηχανισμός αυθεντικοποίησης που προτείνεται για το συγκεκριμένο επίπεδο, αξιοποιεί ψηφιακά πιστοποιητικά, που θα εκδίδονται από την κατάλληλη Υποδομή Δημόσιου Κλειδιού (*PKI*) και την Αρχή Χρονοσήμανσης (*Time stamping Authority*) - Αρχή Πιστοποίησης (*Certification Authority*) . Επιπρόσθετα, προτείνεται η αξιοποίηση διακριτικών χαλαρής ή σκληρής αποθήκευσης. Τα διακριτικά αποθήκευσης θα πρέπει να προστατεύονται από τους αντίστοιχους προσωπικούς κωδικούς του χρήστη. Σε αυτό το επίπεδο αυθεντικοποίησης θα πρέπει να διασφαλίζονται, κατ' ελάχιστον, οι ακόλουθες απαιτήσεις ασφάλειας:

- Εμπιστευτικότητα των
  - Δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη (ιδιωτικότητα)
  - Διαπιστευτηρίων του χρήστη
  - Των δεδομένων που αποστέλλονται από στο χρήση στην ηλεκτρονική υπηρεσία
  - Των δεδομένων που ο χρήστης λαμβάνει από την ηλεκτρονική υπηρεσία
- Ακεραιότητα των

    - Δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη
    - Διαπιστευτηρίων του χρήστη
    - Δεδομένων που αποστέλλονται από το χρήστη στην ηλεκτρονική υπηρεσία
    - Δεδομένων που ο χρήστης λαμβάνει από την ηλεκτρονική υπηρεσία
- Αυθεντικότητα υπηρεσίας
- Μη αποποίηση
    - Αποστολής δεδομένων
    - Λήψης δεδομένων
- Υπηρεσίες εποπτείας (*Auditing*)
- Χρονοσήμανση των ενεργειών

5.6 Επίπεδα Εγγραφής

Ο όρος "*εγγραφή μιας οντότητας σε μια υπηρεσία*" αναφέρεται στο σύνολο των διαδικασιών μέσω των οποίων η οντότητα εκδηλώνει ενδιαφέρον χρήσης μιας συγκεκριμένης ηλεκτρονικής υπηρεσίας και παρέχει όλα τα στοιχεία που απαιτούνται για την έγκριση του δικαιώματος αυτού. Για τον προσδιορισμό του κατάλληλου επιπέδου εγγραφής, το ΠΨΑ καθορίζει ότι θα πρέπει να λαμβάνεται υπόψη το επίπεδο εμπιστοσύνης, στο οποίο εντάσσεται η παρεχόμενη υπηρεσία. Πιο συγκεκριμένα, όσο υψηλότερο είναι το επίπεδο εμπιστοσύνης, τόσο υψηλό θα πρέπει να είναι και το επίπεδο εγγραφής, λαμβάνοντας επιπλέον υπόψη και το διακριτικό αυθεντικοποίησης που θα απαιτηθεί για τη διαδικασία αυθεντικοποίησης. Ενδεικτικά, για υπηρεσίες που υποστηρίζουν οικονομικές συναλλαγές δεν θα πρέπει να επιτρέπεται η εγγραφή να πραγματοποιείται μόνο με τη συμπλήρωση μιας ηλεκτρονικής φόρμας, αλλά θα πρέπει να υπάρχει η κατάλληλη διαδικασία, κατά την οποία ο χρήστης αφού αρχικά επιβεβαιώσει τη γνησιότητα της ταυτότητάς του, θα μπορεί να παραλάβει το κατάλληλο διακριτικό αυθεντικοποίησης και περαιτέρω να αξιοποιήσει την υπηρεσία. Για τον προσδιορισμό του κατάλληλου επιπέδου εγγραφής, οι δημόσιες υπηρεσίες θα πρέπει να λάβουν υπόψη το επίπεδο εμπιστοσύνης στο οποίο εντάσσεται η παρεχόμενη υπηρεσία. Όπως έχει ήδη προαναφερθεί, όσο υψηλότερο είναι το επίπεδο εμπιστοσύνης, τόσο υψηλό θα πρέπει να είναι και το επίπεδο εγγραφής, λαμβάνοντας επιπλέον υπόψη και το διακριτικό αυθεντικοποίησης που θα απαιτηθεί για τη διαδικασία αυθεντικοποίησης.

Ενδεικτικά, για υπηρεσίες που υποστηρίζουν οικονομικές συναλλαγές, δεν θα πρέπει να επιτρέπεται η εγγραφή να πραγματοποιείται μόνο με τη συμπλήρωση μιας ηλεκτρονικής φόρμας (όπως πραγματοποιείται στις υπάρχουσες υπηρεσίες ηλεκτρονικής διακυβέρνησης), αλλά θα πρέπει να υπάρχει η κατάλληλη διαδικασία, κατά την οποία ο χρήστης, αφού αρχικά επιβεβαιώσει τη γνησιότητα της ταυτότητάς του, θα μπορεί να παραλάβει το κατάλληλο διακριτικό αυθεντικοποίησης και περαιτέρω να αξιοποιήσει την υπηρεσία.

Στην ενότητα αυτή αποτυπώνονται τα πρότυπα, οι προδιαγραφές και οι διαδικασίες που απαιτούνται για την εγγραφή μιας οντότητας σε μία υπηρεσία ηλεκτρονικής διακυβέρνησης, προκειμένου να ελεγχθεί η πληρότητα, η ορθότητα και η εγκυρότητα των δεδομένων που υποβάλλονται από τον αιτούντα, και να εκδοθεί το κατάλληλο διακριτικό αυθεντικοποίησης για την παροχή πρόσβασης στις παρεχόμενες υπηρεσίες. Σε κάθε περίπτωση θα πρέπει να σημειωθεί ότι το επίπεδο εγγραφής δεν είναι απαραίτητο να ταυτίζεται με τα επίπεδα εμπιστοσύνης ή αυθεντικοποίησης.

Αξίζει να σημειωθεί ότι η επιτυχημένη ολοκλήρωση ενός συγκεκριμένου Επίπεδου Εγγραφής δεν αποκλείει την ανάγκη ολοκλήρωσης των υπολοίπων επιπέδων εγγραφής σε περίπτωση που ο χρήστης επιθυμεί να κάνει χρήση υπηρεσιών που ανήκουν σε αυτά.

5.6.1 Επίπεδο Εγγραφής 0

Ως Επίπεδο Εγγραφής 0 ορίζεται το σύνολο των διαδικασιών που πρέπει να ακολουθήσει ένας χρήστης, προκειμένου να εξασφαλίσει πρόσβαση σε υπηρεσίες που κυρίως παρέχουν πληροφοριακό υλικό. Οι διαδικασίες του Επιπέδου Εγγραφής 0 θα πρέπει να ακολουθηθούν για τις ηλεκτρονικές υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Αυθεντικοποίησης 0. Δεν υπάρχουν απαιτήσεις ασφάλειας για το επίπεδο εγγραφής 0 ούτε απαιτείται μηχανισμός αυθεντικοποίησης.

5.6.2 Επίπεδο Εγγραφής 1

Στο Επίπεδο Εγγραφής 1 εντάσσεται το σύνολο των διαδικασιών που πρέπει να ακολουθήσει ένας χρήστης, για να αποκτήσει πρόσβαση σε υπηρεσίες που επεξεργάζονται προσωπικά δεδομένα (π.χ. δυνατότητα συμπλήρωσης ηλεκτρονικών αιτήσεων και φορμών για την έκδοση κάποιου δημοσίου εγγράφου). Οι διαδικασίες του επιπέδου εγγραφής 1 θα πρέπει να ακολουθηθούν για τις ηλεκτρονικές υπηρεσίες που έχουν υιοθετήσει το επίπεδο αυθεντικοποίησης 1.

Στο συγκεκριμένο επίπεδο εγγραφής θα πρέπει να διασφαλίζονται τα ακόλουθα:

- Εμπιστευτικότητα των

    - Δεδομένων που αποστέλλει ο χρήστης στην Αρχή Εγγραφής
    - Δεδομένων που αποστέλλονται στο χρήστη από την Αρχή Εγγραφής
    - Διαπιστευτηρίων του χρήστη
- Ακεραιότητα των
    - Δεδομένων που αποστέλλει ο χρήστης στην Αρχή Εγγραφής
    - Δεδομένων που αποστέλλονται στο χρήστη από την Αρχή Εγγραφής
    - Διαπιστευτηρίων του χρήστη
- Μη αποποίηση αποστολής και λήψης δεδομένων

Η μη αποποίηση διασφαλίζεται με την υποβολή της αίτησης (συμπεριλαμβανομένων και των δικαιολογητικών) και την έκδοση των απαιτούμενων διαπιστευτηρίων.

Διαδικασία Εγγραφής: Γίνεται χρήση των εξής μηχανισμών αυθεντικοποίησης:

- Συνθηματικά και
- Συνθηματικά μια χρήσης (one-time passwords)

Το ΠΨΑ ορίζει την εξής διαδικασία εγγραφής για το επίπεδο εγγραφής 1. Αρχικά ο χρήστης συμπληρώνει ηλεκτρονικά κάποια αίτηση, η οποία και περιλαμβάνει πεδία στα οποία θα πρέπει να συμπληρώσει τα προσωπικά του στοιχεία (Όνομα, Επίθετο, Ημερομηνία Γέννησης), τα αναγνωριστικά του για τις ηλεκτρονικές υπηρεσίες στις οποίες επιθυμεί να εγγραφεί π.χ. Αριθμός Δελτίου Ταυτότητας, Αριθμός Φορολογικού Μητρώου, ηλεκτρονική διεύθυνση αλληλογραφίας κλπ. Η συμπληρωμένη αίτηση αποστέλλεται ηλεκτρονικά στην Αρχή Εγγραφής, η οποία αποστέλλει σχετικό αίτημα στον εξυπηρετητή της αντίστοιχης υπηρεσίας, προκειμένου ο φορέας να πραγματοποιήσει έλεγχο αναφορικά με:

- Την εγκυρότητα των στοιχείων της υποβληθείσας αίτησης,
- Τη μη ύπαρξη άλλου λογαριασμού για τον αιτούντα χρήστη για το συγκεκριμένο επίπεδο εγγραφής,
- Την εγκυρότητα των αναγνωριστικών.
- Το αν ο αιτών δικαιούται να χρησιμοποιήσει την ηλεκτρονική υπηρεσία που δήλωσε.

Με την ολοκλήρωση του ελέγχου, αποστέλλεται απάντηση στο σχετικό αίτημα, ενημερώνοντας την Αρχή Εγγραφής για το αποτέλεσμα του ελέγχου. Εάν οι απαντήσεις που λάβει η Αρχή Εγγραφής είναι θετικές, δημιουργείται ο αντίστοιχος λογαριασμός χρήστη. Στη συνέχεια ο χρήστης ενημερώνεται στη διεύθυνση αλληλογραφίας, του με συστημένη επιστολή, για το όνομα χρήστη (*Username*) και το συνθηματικό (*Password*) που θα πρέπει να χρησιμοποιεί προκειμένου

να αυθεντικοποιείται και να κάνει χρήση των ηλεκτρονικών υπηρεσιών που δήλωσε. Μετά την υποβολή της ηλεκτρονικής αίτησης, ο χρήστης λαμβάνει ένα αντίγραφο στη διεύθυνση του ηλεκτρονικού του ταχυδρομείου, το οποίο λειτουργεί ως αποδεικτικό των στοιχείων της αίτησης που έχει υποβάλει. Σε περίπτωση που η Αρχή Εγγραφής διαπιστώσει ότι ο φορέας, για κάποιο συγκεκριμένο λόγο, δεν έκανε δεκτή την αίτηση, ενημερώνει σχετικά το χρήστη στη διεύθυνση αλληλογραφίας του ότι η αίτησή του απορρίφθηκε, εξηγώντας ταυτόχρονα την ακριβή αιτία. Ανεξαρτήτως του επιπέδου εγγραφής, η Αρχή Εγγραφής καταγράφει την αίτηση του χρήστη, χωρίς όμως να αποθηκεύει κάποιο από τα στοιχεία ή αναγνωριστικό του χρήστη.

5.6.3 Επίπεδο Εγγραφής 2

Το Επίπεδο Εγγραφής 2 ορίζει τις διαδικασίες που απαιτούνται για την εγγραφή σε υπηρεσίες αντίστοιχες με αυτές που επιπέδου 1, με τη διαφορά ότι τώρα το έγγραφο / πιστοποιητικό που αιτείται ο χρήστης μπορεί να του αποσταλεί ηλεκτρονικά. Οι διαδικασίες του Επιπέδου Εγγραφής 2 θα πρέπει να ακολουθηθούν για τις ηλεκτρονικές υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Αυθεντικοποίησης 1.

Στο συγκεκριμένο επίπεδο εγγραφής θα πρέπει να διασφαλίζονται τα ακόλουθα:

- Εμπιστευτικότητα των
    - Δεδομένων που αποστέλλει ο χρήστης στην Αρχή Εγγραφής
    - Δεδομένων που αποστέλλονται στο χρήστη από την Αρχή Εγγραφής
    - Διαπιστευτηρίων του χρήστη
- Ακεραιότητα των
    - Δεδομένων που αποστέλλει ο χρήστης στην Αρχή Εγγραφής
    - Δεδομένων που αποστέλλονται στο χρήστη από την Αρχή Εγγραφής
    - Διαπιστευτηρίων του χρήστη
- Μη αποποίηση
    - Αποστολής και λήψης δεδομένων
    - Συμμετοχής σε ηλεκτρονικές συναλλαγές

Για το επίπεδο εγγραφής 2, αρχικά ο χρήστης συμπληρώνει μια αίτηση αντίστοιχη του επιπέδου εγγραφής 1. Η αίτηση αποστέλλεται στην Αρχή Εγγραφής, με στόχο τη διενέργεια των ίδιων ελέγχων, και αντίγραφο της ηλεκτρονικής αίτησης αποστέλλεται και στον αιτούντα ως αποδεικτικό των στοιχείων που δηλώθηκαν. Αν οι έλεγχοι ολοκληρωθούν επιτυχώς, δημιουργείται ο

λογαριασμός του χρήστη και εκδίδεται το διακριτικό συνθηματικών μιας χρήσης, εφόσον δεν έχει ήδη εκδοθεί άλλο και ο χρήστης δεν έχει αναφέρει κλοπή ή δυσλειτουργία του.

Μέσα σε ένα προκαθορισμένο χρονικό διάστημα από την υποβολή της αίτησης, ο χρήστης μπορεί να παραλάβει από την αρμόδια υπηρεσία το κατάλληλο διακριτικό αυθεντικοποίησης, αφού πρώτα ταυτοποιηθεί - αυθεντικοποιηθεί στον αρμόδιο υπάλληλο, επιδεικνύοντας δημόσια έγγραφα που αναγράφουν τα αναγνωριστικά του, το δελτίο της αστυνομικής του ταυτότητας, το αντίγραφο της ηλεκτρονικής αίτησης που υπέβαλε, καθώς και ένα δημόσιο έγγραφο που να αποδεικνύει τη διεύθυνση μόνιμης κατοικίας του.

5.6.4 Επίπεδο Εγγραφής 3

Το Επίπεδο Εγγραφής 3 ορίζει τις διαδικασίες που απαιτούνται για την εγγραφή σε υπηρεσίες που επεξεργάζονται ευαίσθητα προσωπικά δεδομένα ή οικονομικά δεδομένα. Οι διαδικασίες του Επιπέδου Εγγραφής 3 θα πρέπει να ακολουθηθούν για τις ηλεκτρονικές υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Αυθεντικοποίησης 2. Όμοια με όσα ισχύουν για το επίπεδο εγγραφής 2, στο συγκεκριμένο επίπεδο εγγραφής θα πρέπει να διασφαλίζονται τα ακόλουθα:

- Εμπιστευτικότητα των
    - Δεδομένων που αποστέλλει ο χρήστης στην Αρχή Εγγραφής
    - Δεδομένων που αποστέλλονται στο χρήστη από την Αρχή Εγγραφής
    - Διαπιστευτηρίων του χρήστη
- Ακεραιότητα των
    - Δεδομένων που αποστέλλει ο χρήστης στην Αρχή Εγγραφής
    - Δεδομένων που αποστέλλονται στο χρήστη από την Αρχή Εγγραφής
    - Διαπιστευτηρίων του χρήστη
- Μη αποποίηση
    - Αποστολής και λήψης δεδομένων
    - Συμμετοχής σε ηλεκτρονικές συναλλαγές

Οι διαδικασίες είναι αντίστοιχες με αυτές των επιπέδων 1 και 2. Σε αντιστοιχία με τα προηγούμενα επίπεδα, ο χρήστης συμπληρώνει την ηλεκτρονική αίτηση, η οποία θα πρέπει να εγκριθεί από την Αρχή Εγγραφής. Μετά τη έγκριση, δημιουργείται ο λογαριασμός του χρήστη, ενώ η αίτηση προωθείται στην Αρχή Πιστοποίησης, η οποία είναι υπεύθυνη για την έκδοση των ψηφιακών πιστοποιητικών. Μέσα σε ένα προκαθορισμένο χρονικό διάστημα, ο χρήστης θα μπο-

ρεί να παραλαμβάνει το αντίστοιχο διακριτικό αυθεντικοποίησης από την αρμόδια υπηρεσία, αφού πρώτα ταυτοποιηθεί στον αρμόδιο υπάλληλο, επιδεικνύοντας δημόσια έγγραφα αντίστοιχα με αυτά του επιπέδου 2. Μετά την παραλαβή του διακριτικού αυθεντικοποίησης, και σε προκαθορισμένο χρονικό διάστημα, ο προσωπικός κωδικός πρόσβασης (*PIN – Personal Identification Number*) του διακριτικού αποστέλλεται με συστημένη επιστολή στη διεύθυνση αλληλογραφίας του χρήστη.

5.7 Οδηγίες Εφαρμογής Πλαισίου Ψηφιακής Αυθεντικοποίησης

Στην ενότητα αυτή περιλαμβάνονται οδηγίες για την εφαρμογή του Πλαισίου Ψηφιακής Αυθεντικοποίησης από τους δημόσιους φορείς και οργανισμούς. Είναι σκόπιμο οι οδηγίες αυτές να ακολουθούνται τόσο στα πρώτα στάδια ανάπτυξης μιας ηλεκτρονικής υπηρεσίας όσο και κατά τη διάρκεια της παραγωγικής λειτουργίας της.

5.7.1 Κατηγοριοποίηση Δεδομένων

Η προτεινόμενη κατηγοριοποίηση των δεδομένων που δυνητικά μπορούν να αξιοποιηθούν σε μια ηλεκτρονική υπηρεσία, όπως παρουσιάζεται στον Πίνακας 5-4 παρακάτω, έχει βασιστεί στις αντίστοιχες κατηγοριοποιήσεις που έχουν υιοθετήσει:

- η εθνική νομοθεσία (ν. 2472/97 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα),
- η κοινοτική νομοθεσία (Οδηγία 95/46/ΕΚ για την προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών) και
- η διεθνής νομοθεσία (Σύμβαση 108 του Συμβουλίου της Ευρώπης για την προστασία του ατόμου έναντι της αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η οποία ισχύει ως εσωτερικό δίκαιο).

Επιπλέον έχουν ληφθεί υπόψη απόρρητα τα οποία κατοχυρώνονται νομοθετικά, όπως το φορολογικό και ιατρικό απόρρητο.

ΚΑΤΗΓΟΡΙΑ ΔΕΔΟΜΕΝΩΝ: «ΑΠΛΑ ΔΕΔΟΜΕΝΑ»		
Περιγραφή Δεδομένων	**Νομική Βάση**	**Αντιμετώπιση ως προς το Επίπεδο Εμπιστοσύνης**
Κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο, η ταυτότητα του οποίου είναι γνωστή ή μπορεί να διαπιστωθεί. *Λόγω της ευρύτητας του ορισμού δεν είναι δυνατός ο ακριβής προσδιορισμός των δεδομένων που εντάσσονται στα «απλά»*	Άρθρο 2α ν. 2472/97 Ορισμός δεδομένων	Με την επιφύλαξη α) της ένταξης ορισμένων από τα αναφερόμενα στον πίνακα 1) στο προστατευτικό πεδίο απορρήτων, όπως το φορολογικό απόρρητο και
	Άρθρο 5 ν. 2690/99 (ΚΔΔ - Εξαιρέσεις από πρόσβαση σε διοικητικά έγγραφα για την προστασία της ιδιωτικής ζωής ή οικογενειακής ζωής)	β) του ενδεχόμενου να εντάσσονται ορισμένα απλά δεδομένα στο πεδίο της ιδιωτικής ή οικογενειακής ζωής σύμφωνα με τον ΚΔΔ
Ενδεικτικά πρόκειται για **Στοιχεία για τον προσδιορισμό της ταυτότητας του προσώπου.** Με το σύνηθες προσδιοριστικό της ταυτότητας ενός προσώπου, το όνομα, μπορούν να εξομοιωθούν ο αριθμός της κοινωνικής ασφάλισης, ο αριθμός δελτίου ταυτότητας, ο αριθμός πελάτη και άλλα παρόμοια στοιχεία. Ως στοιχεία που δηλώνουν την ταυτότητα ενός προσώπου έχουν γίνει αποδεκτά και νομιμοποιητικά στοιχεία που αποδίδονται σε πρόσωπα ή επιλέγονται από αυτά (κωδικός αναγνώρισης ή πρόσβασης, PIN κ.α.).	Ν. 2472/97	Τηρουμένων των προϋποθέσεων και εγγυήσεων επεξεργασίας που εισάγει ο νόμος 2472/97 και ιδίως τα άρθρα 4, 5 και 6 τα **απλά δεδομένα** μπορούν καταρχήν να ενταχθούν στο επίπεδο εμπιστοσύνης 1, 2

ΚΑΤΗΓΟΡΙΑ ΔΕΔΟΜΕΝΩΝ: «ΑΠΛΑ ΔΕΔΟΜΕΝΑ»		
Περιγραφή Δεδομένων	**Νομική Βάση**	**Αντιμετώπιση ως προς το Επίπεδο Εμπιστοσύνης**
Πληροφορίες που αφορούν – **προσωπική ή/και οικογενειακή κατάσταση**		Τα δεδομένα που αφορούν την **προσωπική ή οικογενειακή κατάσταση** μπορεί να ενταχθούν σε υψηλότερο επίπεδο εμπιστοσύνης, καθώς νομολογιακά έχει κριθεί ότι εμπίπτουν στην κατηγορία του ιδιωτικού βίου
Επάγγελμα - Επαγγελματικές ιδιότητες- **Επαγγελματικές** σχέσεις **Οικονομικές σχέσεις** **Οικονομικά στοιχεία – περιουσιακή κατάσταση**		Για τα **οικονομικά στοιχεία** βλ. και στην ειδική κατηγορία του πίνακα
Έννομες σχέσεις και καταστάσεις δημοσίου και ιδιωτικού δικαίου, όπως - σχέσεις προς πράγματα (κινητά και ακίνητα) - συμβατικές σχέσεις - εκπλήρωση υποχρεώσεων έναντι του δημοσίου/τρίτων (φορολογική και ασφαλιστική ενημερότητα) - διοικητικές άδειες κ.λπ.		

Πίνακας 5-2: Κατηγοριοποίηση Απλών Δεδομένων ανά Νομική Βάση Επεξεργασίας

ΚΑΤΗΓΟΡΙΑ ΔΕΔΟΜΕΝΩΝ: «ΕΥΑΙΣΘΗΤΑ»		
Περιγραφή Δεδομένων	**Νομική Βάση**	**Αντιμετώπιση ως προς το Επίπεδο Εμπιστοσύνης**
Πρόκειται για δεδομένα που αφορούν	Άρθρο 2β ν. 2472/97 Ορισμός ευαίσθητων δεδομένων	Η ρητή ένταξη των δεδομένων αυτών σε κατηγορία αναβαθμισμένης προστασίας επιτάσσει την ένταξή τους στο ανώτερο επίπεδο εμπιστοσύνης
Φυλετική ή Εθνική προέλευση (όχι ιθαγένεια) Τα πολιτικά φρονήματα Θρησκευτικές ή φιλοσοφικές πεποιθήσεις Συμμετοχή σε συνδικαλιστική οργάνωση Την κοινωνική πρόνοια (θα μπορούσαν να θεωρηθούν δεδομένα οικονομικού χαρακτήρα – αφορούν κυρίως την ιδιότητα «πτωχού» - χρήζοντος κοινωνικής υποστήριξης και συνακόλουθα του λήπτη παροχών κοινωνικής πρόνοιας) Ερωτική ζωή, Ποινικές διώξεις ή καταδίκες Συμμετοχή σε ενώσεις προσώπων που μπορεί να σχετίζεται με ή να αποκαλύπτει ευαίσθητα δεδομένα		
Υγείας (Ιατρικά δεδομένα - *Medical Data*) νοούνται όλα τα δεδομένα όσα έχουν μία σαφή και στενή σχέση με την υγεία (παρελθούσα, παρούσα και μέλλουσα κατάσταση). Ως δεδομένα υγείας νοούνται και όσα παρέχουν μία εκτίμηση για την κατάσταση της υγείας ενός προσώπου.		Η ένταξη των δεδομένων αυτών στο ανώτερο επίπεδο εμπιστοσύνης απορρέει και από τις ρυθμίσεις για το ιατρικό απόρρητο που περιέχονται στον Κώδικα Ιατρικής Δεοντολογίας (άρθρο 13 ν. 3418/2005)

Πίνακας 5-3: Κατηγοριοποίηση Ευαίσθητων Δεδομένων ανά Νομική Βάση Επεξεργασίας

ΚΑΤΗΓΟΡΙΑ ΔΕΔΟΜΕΝΩΝ: «ΟΙΚΟΝΟΜΙΚΑ ΔΕΔΟΜΕΝΑ»		
Περιγραφή Δεδομένων	**Νομική Βάση**	**Αντιμετώπιση ως προς το Επίπεδο Εμπιστοσύνης**
Τα οικονομικά δεδομένα, σύμφωνα με την τυπολογία και κατηγοριοποίηση της νομοθεσίας για την προστασία προσωπικών δεδομένων, εντάσσονται στα απλά δεδομένα	Άρθρο 2 α ν. 2472/97	Ένταξη σε συνήθη επίπεδα εμπιστοσύνης
Ωστόσο ορισμένα από αυτά τα δεδομένα καλύπτονται από το φορολογικό απόρρητο και συνεπώς θα πρέπει να αντιμετωπίζονται διαφορετικά	Άρθρο 85 Κώδικα Φορολογίας Εισοδήματος	Τα καλυπτόμενα από το φορολογικό απόρρητο στοιχεία, δηλ. «οι φορολογικές δηλώσεις, τα φορολογικά στοιχεία, οι εκθέσεις και κάθε άλλο στοιχείο του φακέλου που έχει σχέση με τη φορολογία ή άπτεται αυτής» θα πρέπει να εντάσσονται στο ανώτερο επίπεδο εμπιστοσύνης

Πίνακας 5-4: Κατηγοριοποίηση Οικονομικών Δεδομένων ανά Νομική Βάση Επεξεργασίας

5.7.2 Οδηγίες Προσδιορισμού Επιπέδου Εμπιστοσύνης

Για τον προσδιορισμό του επιπέδου εμπιστοσύνης, ο φορέας θα πρέπει:

1. Να προσδιορίσει τα δεδομένα που επεξεργάζεται η υπηρεσία και να τα κατατάξει (με βάση τους Πίνακας 5-2, Πίνακας 5-3 & Πίνακας 5-4) σε μια από τις παρακάτω κατηγορίες:
    i. Απλά (Συμπεριλαμβάνονται και τα "Δημόσια" προσπελάσιμα δεδομένα)
    ii. Οικονομικά
    iii. Ευαίσθητα
2. Να προσδιορίσει το επίπεδο εμπιστοσύνης στο οποίο θα ενταχθεί η προσφερόμενη υπηρεσία, λαμβάνοντας υπόψη ότι:
    i. Όσες ηλεκτρονικές υπηρεσίες αξιοποιούν απλά δεδομένα εντάσσονται στο:
        α. Επίπεδο Εμπιστοσύνης 0, εφόσον τα δεδομένα αφορούν δημόσια προσπελάσιμες πληροφορίες (ανακοινώσεις, αιτήσεις) και γενικώς δεδομένα που είναι αδύνατον να συσχετισθούν με κάποιο άτομο-πολίτη.
        β. Επίπεδο Εμπιστοσύνης 1, εφόσον αφορούν δεδομένα που αναφέρονται σε φυσικό πρόσωπο, η ταυτότητα του οποίου είναι γνωστή ή μπορεί να διαπιστωθεί, και δεν γίνεται επεξεργασία αναγνωριστικών του χρήστη (όπως Αριθμός Δελτίου Ταυτότητας, Αριθμός Φορολογικού Μητρώου κτλ) για την παροχή της υπηρεσίας.
        γ. Επίπεδο Εμπιστοσύνης 3, εφόσον αφορούν δεδομένα που αναφέρονται σε φυσικό πρόσωπο, η ταυτότητα του οποίου είναι γνωστή ή μπορεί να διαπιστωθεί, και γίνεται επεξεργασία αναγνωριστικών του χρήστη (όπως Αριθμός Δελτίου Ταυτότητας, Αριθμός Φορολογικού Μητρώου κτλ) για την παροχή της υπηρεσίας. Επίσης, στο Επίπεδο Εμπιστοσύνης 2 εντάσσονται όλες οι υπηρεσίες που αξιοποιούν οικονομικά δεδομένα που δεν εντάσσονται στο φορολογικό απόρρητο και αφορούν οικονομικές συναλλαγές προκαθορισμένου ύψους, καθώς και υπηρεσίες που αξιοποιούν απλά δεδομένα και δεν μπορούν (σύμφωνα με τα παραπάνω) να ενταχθούν

στα Επίπεδα Εμπιστοσύνης 0 ή 1 (για παράδειγμα πληροφορίες που θεωρείται ότι αφορούν τον ιδιωτικό ή/και οικογενειακό βίο του ατόμου).

ii. Όσες υπηρεσίες αξιοποιούν οικονομικά δεδομένα:

α. Αν τα δεδομένα δεν υπάγονται στα φορολογικό απόρρητο και αφορούν οικονομικές συναλλαγές προκαθορισμένου ύψους, τότε θεωρούνται "Απλά Δεδομένα" και εντάσσονται στο Επίπεδο Εμπιστοσύνης 2.

β. Αν τα δεδομένα αφορούν οικονομικές συναλλαγές μη προκαθορισμένου ύψους, εντάσσονται στο Επίπεδο Εμπιστοσύνης 3

γ. Αν τα δεδομένα υπάγονται στο φορολογικό απόρρητο, εντάσσονται στο επίπεδο εμπιστοσύνης 3.

iii. Όσες ηλεκτρονικές υπηρεσίες αξιοποιούν ευαίσθητα δεδομένα, εντάσσονται στο Επίπεδο Εμπιστοσύνης 3.

5.7.3 Συσχετισμός Επιπέδων Εμπιστοσύνης, Αυθεντικοποίησης και Εγγραφής

Στον Πίνακας 5-5, που ακολουθεί, παρουσιάζεται ο συσχετισμός μεταξύ επιπέδων εμπιστοσύνης, αυθεντικοποίησης και εγγραφής και θα πρέπει να λαμβάνεται υπ' όψιν κατά την επιλογή των επιπέδων αυθεντικοποίησης και εγγραφής αφού προηγουμένως έχει προσδιοριστεί το αντίστοιχο επίπεδο εμπιστοσύνης.

Επίπεδο Εμπιστοσύνης	**Επίπεδο Εγγραφής**	**Επίπεδο Αυθεντικοποίησης**	**Μηχανισμός Αυθεντικοποίησης**
0	0	0	-
1	1	1	Συνθηματικά
2	2		Συνθηματικά μιας Χρήσης
3	3	2	Πιστοποιητικά (Διακριτικό Χαλαρής Αποθήκευσης)
			Πιστοποιητικά (Διακριτικό Σκληρής Αποθήκευσης)

Πίνακας 5-5: Αντιστοίχηση Επιπέδων Εγγραφής, Αυθεντικοποίησης & Εμπιστοσύνης

Συγκεκριμένα:

- για υπηρεσίες Επιπέδου Εμπιστοσύνης 0, δεν απαιτούνται διαδικασίες εγγραφής και αυθεντικοποίησης.
- για υπηρεσίες Επιπέδου Εμπιστοσύνης 1 & 2, μπορούν να αξιοποιηθούν είτε συνθηματικά είτε συνθηματικά μιας χρήσης σε περιπτώσεις που ο φορέας κρίνει ότι απαιτείται μεγαλύτερος βαθμός βεβαιότητας αναφορικά με την ορθότητα της ψηφιακής ταυτότητας του χρήστη. Σε αυτή την περίπτωση το επίπεδο εγγραφής που θα υιοθετεί η υπηρεσία θα είναι το 2, έτσι ώστε και η διαδικασία εγγραφής να ελαχιστοποιεί τις πιθανότητες μια οντότητα να υποδυθεί μια άλλη.
- όσες υπηρεσίες εντάσσονται στο Επίπεδο Εμπιστοσύνης 3, ακολουθούν διαδικασίες εγγραφής επιπέδου 3 αποκλειστικά, ενώ η αυθεντικοποίηση των χρηστών πραγματοποιείται με την αξιοποίηση των αντίστοιχων ψηφιακών πιστοποιητικών. Τα πιστοποιητικά των χρηστών είναι δυνατόν να διανέμονται είτε σε διακριτικά χαλαρής αποθήκευσης είτε σε σκληρής αποθήκευσης. Η επιλογή γίνεται από το φορέα, ο οποίος, εφόσον επιθυμεί να πληρούνται οι προϋποθέσεις της νομικά κατοχυρωμένης ισοδυναμίας της ιδιόχειρης υπογραφής με την ψηφιακή, δηλαδή να καλύπτονται οι απαιτήσεις του Π.Δ. 150/2001, θα πρέπει να επιλέξει διακριτικά σκληρής αποθήκευσης.

5.8 Οδηγίες προς Φυσικά και Νομικά Πρόσωπα

5.8.1 Αρχική Εγγραφή σε Ηλεκτρονική Υπηρεσία

Προκειμένου ο χρήστης, φυσικό η νομικό πρόσωπο, να μπορέσει να κάνει χρήση μιας ή περισσότερων ηλεκτρονικών υπηρεσιών θα πρέπει να ολοκληρώσει ένα σύνολο διαδικασιών, ανάλογα με το επίπεδο εμπιστοσύνης που εντάσσεται η κάθε υπηρεσία και συνεπώς με το αντίστοιχο επίπεδο εγγραφής, προκειμένου να είναι σε θέση να ταυτοποιείται και να αυθεντικοποιείται επιτυχώς από την ΚΔΠ.

Ο χρήστης, για να αξιοποιήσει μία ηλεκτρονική υπηρεσία, αρχικά θα πρέπει να εγγραφεί σε αυτήν. Οι ενέργειες που θα πρέπει να πραγματοποιηθούν για την επιτυχή εγγραφή ενός χρήστη είναι οι ακόλουθες:

- Επιλογή της υπηρεσίας στην οποία επιθυμεί να εγγραφεί, από σύνολο διαθέσιμων επιλογών στο Διαδικτυακό τόπο της ΚΔΠ
- Υποβολή ηλεκτρονικής αίτησης στο Διαδικτυακό τόπο της ΚΔΠ, για την ηλεκτρονική υπηρεσία στην οποία επιθυμεί να εγγραφεί. Στην αίτηση συμπεριλαμβάνεται η συμπλήρωση της κατά περίπτωση προβλεπόμενης αντίστοιχης ηλεκτρονικής φόρμας.
- Κατά περίπτωση ηλεκτρονική υποβολή ή απευθείας κατάθεση των απαιτουμένων δικαιολογητικών για την ολοκλήρωση της εγγραφής στην υπηρεσία, όπως αυτά θα έχουν προσδιοριστεί από το φορέα, με βάση το επίπεδο εμπιστοσύνης που θα έχει αποφασίσει να εντάξει τη συγκεκριμένη ηλεκτρονική υπηρεσία.

Με την ολοκλήρωση των ενεργειών αυτών, η ΚΔΠ μεριμνά για τη λήψη των υποβληθέντων στοιχείων και τον έλεγχο της ορθότητας και της πληρότητάς τους, ενώ ακολούθως ενημερώνει τον ενδιαφερόμενο για την επιτυχή ή μη εγγραφή του στην υπηρεσία. Επί θετικής εκβάσεως, με βάση το επίπεδο εμπιστοσύνης της ηλεκτρονικής υπηρεσίας, του αποστέλλει ή τον καλεί να παραλάβει τα αντίστοιχα διακριτικά αυθεντικοποίησης, τα οποία απαιτούνται για την προσπέλαση στην υπηρεσία.

Κατά την αρχική εγγραφή του χρήστη θα προσφέρεται η δυνατότητα για ταυτόχρονη εγγραφή σε περισσότερες από μία υπηρεσίες. Στην περίπτωση αυτή μπορεί να παρέχεται η δυνατότητα στον αιτούντα της επιλογής έκδοσης i) είτε μόνο του "ισχυρότερου" διαπιστευτηρίου αυθεντικοποίησης, με βάση το υψηλότερο επίπεδο εμπιστοσύνης στο οποίο εντάσσεται κάποια από τις υπηρεσίες που αιτήθηκε, ii) είτε, εναλλακτικά, διαφορετικών διαπιστευτηρίων αυθεντικοποίησης, ισάριθμων με τα διαφορετικά επίπεδα εμπιστοσύνης στα οποία εντάσσονται οι υπηρεσίες τις οποίες αιτήθηκε (ένα διακριτικό αυθεντικοποίησης, ανά επίπεδο εμπιστοσύνης).

5.8.2 Αίτηση για Αξιοποίηση Νέας Υπηρεσίας

Σε περίπτωση που ο χρήστης επιθυμεί να εγγραφεί σε κάποια νέα ηλεκτρονική υπηρεσία, θα πρέπει να πραγματοποιήσει τα ακόλουθα:

- Επιλογή της νέας υπηρεσίας στην οποία επιθυμεί να εγγραφεί, από σύνολο διαθέσιμων επιλογών στο Διαδικτυακό τόπο της ΚΔΠ
- Υποβολή ηλεκτρονικής αίτησης στο Διαδικτυακό τόπο της ΚΔΠ, για τη νέα ηλεκτρονική υπηρεσία στην οποία επιθυμεί να εγγραφεί. Στην αίτηση συμπεριλαμβά-

νεται η συμπλήρωση της κατά περίπτωση προβλεπόμενης αντίστοιχης ηλεκτρονικής φόρμας.

- Κατά περίπτωση ηλεκτρονική υποβολή ή απευθείας κατάθεση των απαιτουμένων δικαιολογητικών για την ολοκλήρωση της εγγραφής στη νέα υπηρεσία, όπως αυτά θα έχουν προσδιοριστεί από το φορέα, με βάση το επίπεδο εμπιστοσύνης που θα έχει αποφασίσει να εντάξει τη συγκεκριμένη ηλεκτρονική υπηρεσία.

Το τμήμα της ΚΔΠ που είναι υπεύθυνο για την εγγραφή των χρηστών, σε κάθε αίτηση εγγραφής που δέχεται, ελέγχει, εάν έχουν εκδοθεί διακριτικά αυθεντικοποίησης για τον αιτούντα για το επίπεδο στο οποίο ανήκει η νέα υπηρεσία που επιθυμεί να εγγραφεί. Σε περίπτωση που δεν έχουν εκδοθεί διακριτικά αυθεντικοποίησης για το συγκεκριμένο επίπεδο εμπιστοσύνης στο οποίο εντάσσεται η νέα υπηρεσία, η αρμόδια αρχή της ΚΔΠ εκδίδει τα αντίστοιχα διακριτικά και τα αποστέλλει στο χρήστη, με τρόπο παράδοσης ο οποίος διαφοροποιείται ανάλογα με τον τύπο των διακριτικών. Σε διαφορετική περίπτωση, αν ο χρήστης έχει παραλάβει από προηγούμενη διαδικασία εγγραφής διακριτικά αυθεντικοποίησης για το συγκεκριμένο επίπεδο εμπιστοσύνης που είναι ενταγμένη η νέα υπηρεσία, δεν παραλαμβάνει νέα διαπιστευτήρια, αλλά αξιοποιεί τα υπάρχοντα για τη χρήση της νέας αυτής υπηρεσίας, αμέσως μόλις η ΚΔΠ ενεργοποιήσει τη σχετική δυνατότητα για αυτόν.

5.8.3 Χρήση Υπηρεσίας

Χρήση κάποιας ηλεκτρονικής υπηρεσίας μπορεί να επιτευχθεί, μόνον εφόσον ο αιτών έχει ολοκληρώσει επιτυχώς τη διαδικασία εγγραφής και αφού πραγματοποιήσει τα ακόλουθα βήματα:

- Επίσκεψη στο Διαδικτυακό τόπο της ΚΔΠ
- Επιλογή της ηλεκτρονικής υπηρεσίας την οποία επιθυμεί να χρησιμοποιήσει και στην οποία προφανώς έχει ήδη εγγραφεί κατά το παρελθόν
- Εισαγωγή του απαιτούμενου για την ταυτοποίηση αναγνωριστικού και για την αυθεντικοποίηση διακριτικού

5.8.4 Ανάκληση Εγγραφής σε Ηλεκτρονική Υπηρεσία

Προκειμένου κάποιος πολίτης να αιτηθεί ανάκλησης εγγραφής σε μία ηλεκτρονική υπηρεσία θα πρέπει να προβεί στις ακόλουθες ενέργειες:

- Επίσκεψη στο Διαδικτυακό τόπο της ΚΔΠ

- Εισαγωγή του απαιτούμενου για την ταυτοποίηση αναγνωριστικού και για την αυθεντικοποίηση διακριτικού, ανάλογα με το επίπεδο εμπιστοσύνης της προς ανάκληση ηλεκτρονικής υπηρεσίας
- Επιλογή της συγκεκριμένης υπηρεσίας, για την οποία επιθυμεί να ανακαλέσει την εγγραφή του (ενδεχομένως να παρέχεται η δυνατότητα στον αιτούντα να ανακαλέσει τη δυνατότητά του χρήσης μίας ηλεκτρονικής υπηρεσίας, ακόμη και αν αυθεντικοποιηθεί με διακριτικό που αντιστοιχεί σε υψηλότερο επίπεδο εμπιστοσύνης από την προς ανάκληση υπηρεσία)
- Επιβεβαίωση της πρόθεσής του να ανακαλέσει τη χρήση της συγκεκριμένης ηλεκτρονικής υπηρεσίας

ΚΕΦΑΛΑΙΟ 6 - ΠΟΛΙΤΙΚΕΣ ΚΑΙ ΠΡΟΤΙΜΗΣΕΙΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Στο παρόν κεφάλαιο εξετάζεται για πρώτη φορά η αξιοποίηση των Πολιτικών και των Προτιμήσεων Ιδιωτικότητας σε σύγχρονα Π.Σ. Ηλεκτρονικής Διακυβέρνησης και προτείνεται μία ολοκληρωμένη αρχιτεκτονική ενσωμάτωσης, με στόχο την απλούστευση παροχής ηλεκτρονικών υπηρεσιών, διασφαλίζοντας παράλληλα ότι οι τελικοί χρήστες διατηρούν τον απαραίτητο έλεγχο για τη συλλογή, επεξεργασία και αποθήκευση των προσωπικών τους δεδομένων, καθώς και τη διαβεβαίωση για την τήρηση των αντίστοιχων νομικών και κανονιστικών υποχρεώσεων από την πλευρά των παρόχων.

6.1 Τεχνολογίες Προάσπισης της Ιδιωτικότητας

Σύμφωνα με τη μελέτη που διενεργήθηκε για λογαριασμό του Υπουργείου Επιστήμης της Δανίας (Meta, 2005), οι τεχνολογίες προάσπισης της ιδιωτικότητας μπορούν να διαχωριστούν σε δύο βασικές κατηγορίες:

- *Τεχνολογίες για την Προστασία της Ιδιωτικότητας (Privacy Protection)*: αφορά μεθόδους για την προστασία ή/και την απόκρυψη δεδομένων και πληροφορίας
- *Τεχνολογίες για τη Διαχείριση της Ιδιωτικότητας (Privacy Management)*: εφαρμογή μηχανισμών για τον έλεγχο πρόσβασης σε δεδομένα και πληροφορίες και τη χρήση τεχνικών μέσων και συστημάτων που βασίζονται σε πολιτικές και κανόνες για την εφαρμογή των προδιαγεγραμμένων απαιτήσεων.

Καθεμία από αυτές τις κατηγορίες περιλαμβάνει διάφορες υποκατηγορίες εργαλείων λογισμικού και μηχανισμών, οι οποίες παρουσιάζονται στον Πίνακας 6-1 που ακολουθεί:

Κατηγορία	Υποκατηγορίες	Τυπικά Χαρακτηριστικά
Προστασία Ιδιωτικότητας	Εργαλεία Ψευδωνυμίας	Επιτρέπουν την πραγματοποίηση ηλεκτρονικών συναλλαγών (transactions) χωρίς να απαιτείται αποστολή προσωπικών δεδομένων
	Εργαλεία Ανωνυμίας	Επιτρέπουν την πραγματοποίηση ηλεκτρονικών συναλλαγών (transactions) χωρίς να γίνεται γνω-

Κατηγορία	Υποκατηγορίες	Τυπικά Χαρακτηριστικά
		στή η πραγματική ταυτότητα του χρήστη
	Εργαλεία Κρυπτογράφησης	Επιτρέπουν την πραγματοποίηση ηλεκτρονικών συναλλαγών (transactions) χωρίς να γίνονται γνωστά προσωπικά δεδομένα του χρήστη σε μη εξουσιοδοτημένες οντότητες
	Φίλτρα Προστασίας	Αποτρέπουν ανεπιθύμητο περιεχόμενο να κοινοποιηθεί στο χρήστη
	Διαγραφείς Ιστορικού και Πρόσφατης Δραστηριότητας	Απομακρύνουν ηλεκτρονικά ίχνη (electronic traces) από τις δραστηριότητες του χρήστη.
Διαχείριση Ιδιωτικότητας	Εργαλεία Ενημέρωσης	Επιτρέπουν τη δημιουργία και τον έλεγχο των Πολιτικών Ιδιωτικότητας
	Εργαλεία Διαχείρισης	Επιτρέπουν τη διαχείριση της ψηφιακής ταυτότητας του χρήστη και των δικαιωμάτων του

Πίνακας 6-1: Υποκατηγορίες Μηχανισμών και Εργαλείων Λογισμικού για Προάσπιση της Ιδιωτικότητας (Meta, 2005)

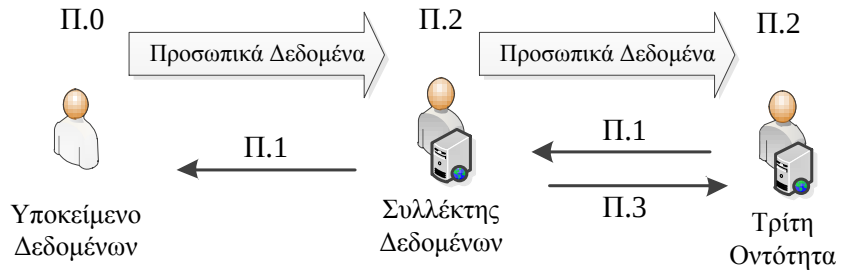
Το βασικό πρόβλημα των τεχνολογιών προστασίας της ιδιωτικότητας είναι ότι προδιαγράφουν "*υποσχέσεις ιδιωτικότητας*" (*Privacy Promises*) χωρίς να περιλαμβάνουν τα μέσα που θα παρέχουν τις εγγυήσεις για την τήρηση των υποσχέσεων (Barth & Mitchell, 2005), (Yee, 2007). Αυτή την αδυναμία έρχονται να καλύψουν οι τεχνολογίες για τη διαχείριση της ιδιωτικότητας και πιο συγκεκριμένα οι δομημένες γλώσσες έκφρασης και εφαρμογής των πολιτικών ιδιωτικότητας. Σύμφωνα με τους (Anderson, 2006), (Λιουδάκης, 2008), οι απαιτήσεις για τέτοιες γλώσσες είναι:

- Να υποστηρίζουν περιορισμούς αναφορικά με τις οντότητες που επιτρέπεται να πραγματοποιούν συγκεκριμένες ενέργειες σε συγκεκριμένους υπολογιστικούς πόρους.
- Να υποστηρίζουν την αντιστοίχηση μεταξύ των σκοπών για τους οποίους πραγματοποιήθηκε η συλλογή και επεξεργασία των δεδομένων, με τους σκοπούς για τους οποίους επιχειρείται η προσπέλασή τους.
- Να υποστηρίζουν προδιαγραφές που περιγράφουν υποκείμενα, πόρους, ενέργειες και συνθήκες πρόσβασης με χρήση αναγνωριστικών τα οποία μπορούν να αντιστοιχηθούν απ' ευθείας σε πραγματικά αντικείμενα και λειτουργίες.

- Να μπορούν να χρησιμοποιηθούν ως πρότυπο ανεξάρτητα από την υπολογιστική πλατφόρμα που εφαρμόζονται.
- Να μπορούν να συσχετιστούν με τη γλώσσα προδιαγραφής πολιτικών ελέγχου πρόσβασης.

6.2 Πολιτικές και Προτιμήσεις Ιδιωτικότητας

Μία Πολιτική Ιδιωτικότητας (*Privacy Policy*) αποτελεί τη δήλωση του παρόχου μιας ηλεκτρονικής υπηρεσίας, σχετικά με τα προσωπικά δεδομένα του τελικού χρήστη που θα αξιοποιηθούν κατά την επιτυχή παροχή της συγκεκριμένης υπηρεσίας (PICOS, 2008). Συνήθως περιέχει πληροφορίες σχετικά με τι προσωπικά δεδομένα θα συλλεχθούν, πώς αυτά θα χρησιμοποιηθούν, για πόσο καιρό θα διατηρηθούν, τις οντότητες στις οποίες θα αποκαλυφθούν καθώς και τα μέτρα ή το βαθμό προστασίας που εφαρμόζεται. Σε ένα απλοϊκό σενάριο, ο χρήστης, το υποκείμενο των δεδομένων, αποκαλύπτει προσωπικά δεδομένα στον πάροχο της υπηρεσίας, που αποτελεί τον συλλέκτη δεδομένων, ο οποίος με τη σειρά του μπορεί να τα μεταβιβάσει σε κάποια τρίτη οντότητα.



Σχήμα 6-1: Τύποι Πολιτικών Ιδιωτικότητας (Madsen et al., 2006)

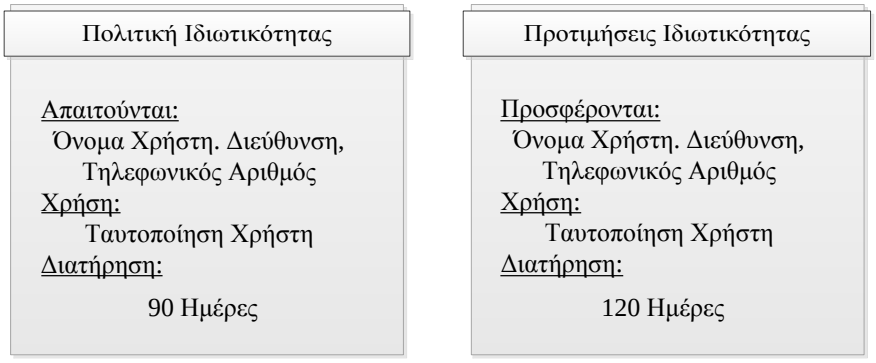
Στο συγκεκριμένο σενάριο, Σχήμα 6-1, διακρίνονται τέσσερεις βασικοί τύποι Πολιτικών Ιδιωτικότητας (Madsen et al., 2006) (Kumaraguru et al., 2007)

- *Προτιμήσεις Ιδιωτικότητας (Π.0)*: Το υποκείμενο των προσωπικών δεδομένων (data subject) περιγράφει και καθορίζει τους όρους και τις προϋποθέσεις βάσει των οποίων προτίθεται να αποκαλύψει (disclose) συγκεκριμένα προσωπικά δεδομένα.
- *Πολιτική Διασφάλισης Ιδιωτικότητας Προσωπικών Δεδομένων (Π.1)*: Ο συλλέκτης των δεδομένων (*Data consumer*) περιγράφει τις διαδικασίες και τους μηχανισμούς διασφάλισης της ιδιωτικότητας που εφαρμόζει καθώς και την αξιοποίηση των προσωπικών δεδομένων .

- *Πολιτική Εσωτερικής Χρήσης Προσωπικών Δεδομένων (Π.2)*: Επιτρέπει στο υποκείμενο των προσωπικών δεδομένων να επιβεβαιώνει τους ισχυρισμούς που έκανε ο συλλέκτης των δεδομένων στο *Π.1*
- *Πολιτική Επεξεργασίας και Επαναχρησιμοποίησης Προσωπικών Δεδομένων (Π.3)*: Σε περίπτωση που τα προσωπικά δεδομένα προωθούνται σε τρίτες οντότητες, διασφαλίζει ότι τηρούνται οι όροι που αναφέρθηκαν κατά την αρχική παραχώρησή τους *(Π.1)*.

Με βάση την παραπάνω κατηγοριοποίηση, διακρίνονται δύο βασικοί τύποι πολιτικών (Kumaraguru et al., 2007) (Wang & Kobsa, 2008):

- *Πολιτικές Ιδιωτικότητας (Privacy Policies)*: μπορούν να χρησιμοποιηθούν για να περιγράψουν τα *Π.1*, *Π.2* και *Π.3*
- *Προτιμήσεις Ιδιωτικότητας (Privacy Preferences)*: μπορούν να χρησιμοποιηθούν για να περιγράψουν το *Π.0*



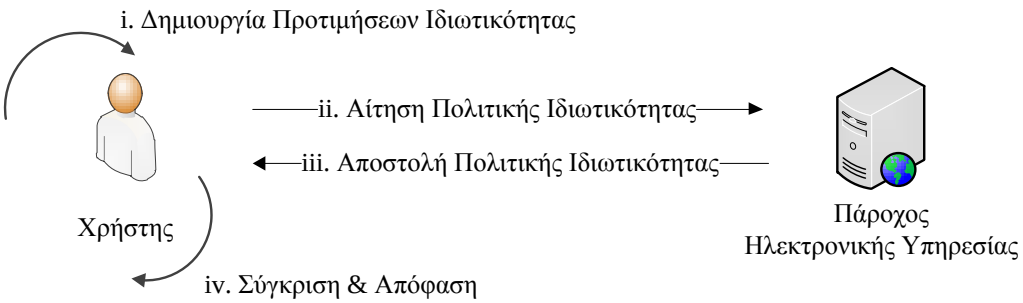
Σχήμα 6-2: Παράδειγμα Πολιτικών και Προτιμήσεων Ιδιωτικότητας

6.2.1 Αξιοποίηση Πολιτικών και Προτιμήσεων Ιδιωτικότητας

Σε ένα παραδοσιακό μοντέλο εφαρμογής των πολιτικών και των προτιμήσεων ιδιωτικότητας, όπως παρουσιάζεται και στο Σχήμα 6-3παρακάτω, ο πάροχος της ηλεκτρονικής υπηρεσίας (*Data collector*) συντάσσει την Πολιτική Ιδιωτικότητάς του και την καθιστά διαθέσιμη στην ιστοσελίδα του ή εναλλακτικά την αποστέλλει στο χρήστη ύστερα από σχετικό αίτημα. Για την παροχή της συγκε-

κριμένης υπηρεσίας ζητά από τον χρήστη (*Data Subject*) να την ελέγξει και να συμφωνήσει στους όρους που περιγράφει..

.



Σχήμα 6-3: Παραδοσιακό Μοντέλο Εφαρμογής Πολιτικών και Προτιμήσεων Ιδιωτικότητας

Ο χρήστης εξετάζει το έγγραφο της πολιτικής, μέσω κάποιου τρίτου λογισμικού, και το συγκρίνει με τις προτιμήσεις ιδιωτικότητάς του. Σε περίπτωση ασυμβατότητας δεν αιτείται την παροχή της υπηρεσίας ενώ σε περίπτωση συμφωνίας, ενημερώνει κατάλληλα τον πάροχο.

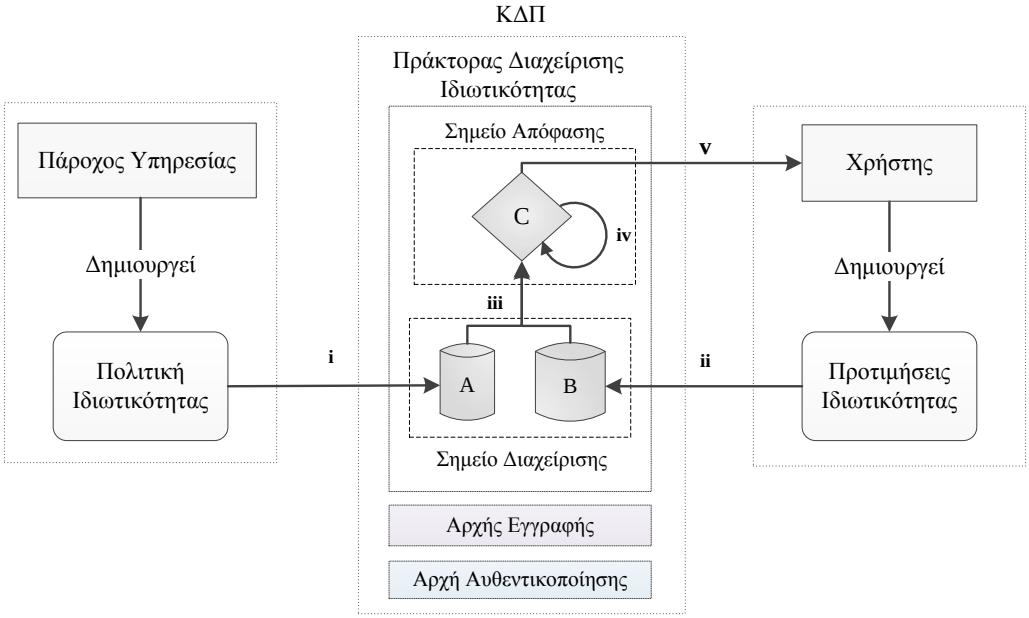
6.2.2 Εφαρμογή σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης

Το συγκεκριμένο μοντέλο θα μπορούσε να αξιοποιηθεί σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης επιτρέποντας την αυτοματοποιημένη παροχή ηλεκτρονικών υπηρεσιών με βάση λεπτομερείς περιγραφές των προτιμήσεων ιδιωτικότητας των χρηστών, οι οποίες μπορούν να μεταβάλλονται κατά το δοκούν (McRobb & Stahl, 2007). Ανεξάρτητα όμως από τα εμφανή οφέλη, υπάρχουν δύο βασικές αδυναμίες. Οι Προτιμήσεις Ιδιωτικότητας των χρηστών δεν μπορούν να διαχειρίζονται από τρίτες εφαρμογές λογισμικού στο φυλλομετρητή (*Browser*), καθώς αποτελούν πιθανό σημείο ευπάθειας (Šilić et al., 2010). Αντίστοιχα, η αποθήκευσή τους τοπικά δεν συμβαδίζει με την απαίτηση για διαθεσιμότητα των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης από οποιοδήποτε σημείο πρόσβασης.

6.3 Πράκτορας Διαχείρισης Ιδιωτικότητας

Τα σύγχρονα Π.Σ. Ηλεκτρονικής Διακυβέρνησης περιλαμβάνουν μία Κεντρική Διαδικτυακή πύλη (ΚΔΠ) που αποτελεί το front-end όλων των παρεχόμενων ηλεκτρονικών υπηρεσιών. Η συγκεκριμένη πύλη ενσωματώνει επίσης και τις Αρχές Εγγραφής και Αυθεντικοποίησης, προκειμένου να καθίσταται δυνατή η παροχή υπηρεσιών (Tambouris & Wimmer, 2005) (Votis et al., 2008) (Gotoh, 2008) (Zhang & Wang, 2008) (Sedek et al., 2011). Παράλληλα με αυτές τις αρχές, προτείνε-

ται η εισαγωγή μιας νέας οντότητας, του Πράκτορα Διαχείρισης της Ιδιωτικότητας (ΠΔΙ). Ο ΠΔΙ θα είναι υπεύθυνος για i) την αποθήκευση των πολιτικών ιδιωτικότητας των παρόχων ηλεκτρονικών υπηρεσιών, ii) την αποθήκευση των προτιμήσεων ιδιωτικότητας των χρηστών και iii) τη σύγκρισή τους. Η δομή του ΠΔΙ παρουσιάζεται στο Σχήμα 6-4 που ακολουθεί:



Σχήμα 6-4: Πράκτορας Διαχείρισης Ιδιωτικότητας

Ο Πράκτορας Διαχείρισης Ιδιωτικότητας (ΠΔΙ) χωρίζεται σε δύο βασικά τμήματα: το Σημείο Διαχείρισης και το Σημείο Απόφασης. Το Σημείο Διαχείρισης απαρτίζεται από δύο αποθετήρια στα οποία αποθηκεύεται η Πολιτική Ιδιωτικότητας κάθε ηλεκτρονικής υπηρεσίας (Αποθετήριο Α) και οι Προτιμήσεις Ιδιωτικότητας κάθε χρήστη (Αποθετήριο Β). Κατά την αρχική εγγραφή μιας ηλεκτρονικής υπηρεσίας στην Κεντρική Διαδικτυακή Πύλη, ο πάροχός της θα πρέπει να υποβάλλει επιπρόσθετα των απαιτούμενων πληροφοριών και την αντίστοιχη Πολιτική Ιδιωτικότητας. Άσχετα από τον συνολικό αριθμό ηλεκτρονικών υπηρεσιών που προσφέρει ο εκάστοτε πάροχος, θα πρέπει να υποβάλλεται ξεχωριστή Πολιτική Ιδιωτικότητας για κάθε ηλεκτρονική υπηρεσίας. Στην πολιτική θα πρέπει να αναφέρονται και να περιγράφονται ρητά τα δεδομένα που απαιτούνται για την παροχή της ηλεκτρονικής υπηρεσίας, ο σκοπός για τον οποίο απαιτούνται, αν θα υποβληθούν σε επεξεργασία, εφόσον αποθηκεύονται, για πόσο καιρό θα αποθηκευθούν και εάν θα κοινοποιηθούν σε τρίτο πάροχο ηλεκτρονικών υπηρεσιών. Μετά την υποβολή της πολιτικής (ενέργεια i Σχήμα 6-4), ο ΠΔΙ επαληθεύ-

ει την προέλευσή της μέσω της ψηφιακής υπογραφής που τη συνοδεύει και την αποθηκεύει στο Αποθετήριο Πολιτικών Ιδιωτικότητας (Α).

Αντίστοιχα, όταν ένας χρήστης εγγράφεται στην ΚΔΠ θα πρέπει να υποβάλλει επιπρόσθετα των απαιτούμενων πληροφοριών και τις Προτιμήσεις Ιδιωτικότητάς του. Οι συγκεκριμένες δεν αφορούν αποκλειστικά μία συγκεκριμένη ηλεκτρονική υπηρεσία, αλλά το σύνολο των προσωπικών δεδομένων του χρήστη και ως εκ τούτου είναι απαραίτητη η υποβολή τους μόνο μία φορά, καθώς αφορούν το σύνολο των διαθέσιμων πληροφοριών. Για κάθε τύπο δεδομένων ο χρήστης θα πρέπει να προσδιορίσει το σκοπό για τον οποίο μπορούν να αξιοποιηθούν από μία ηλεκτρονική υπηρεσία, αν μπορούν να επεξεργασθούν, να αποθηκευθούν και για πόσο χρονικό διάστημα. Εξαιτίας του μεγάλου αριθμού δεδομένων και της διαφορετικής φύσης τους, προτείνεται να υπάρξει ένας βασικός διαχωρισμός σε προσωπικά δεδομένα και προσωπικά αναγνωριστικά (*Personal Identifiers*). Επιπρόσθετα κρίνεται σκόπιμο ο χρήστης να αναφέρει επακριβώς τους παρόχους που δύνανται να τα αξιοποιήσουν, ώστε σε συνδυασμό με τις υπόλοιπες πληροφορίες να μπορεί να αποτυπώσει επακριβώς τις πραγματικές προτιμήσεις του. Μετά την υποβολή του ηλεκτρονικού εγγράφου (ενέργεια ii Σχήμα 6-4), ο ΠΔΙ επιβεβαιώνει την προέλευσή του μέσω της ψηφιακής υπογραφής που το συνοδεύει και το αποθηκεύει στο Αποθετήριο Προτιμήσεων Ιδιωτικότητας (Β). Ωστόσο, καθώς είναι αναμενόμενο ο χρήστης να θελήσει να αναθεωρήσει τις προτιμήσεις του, μπορεί να υποβάλει εκ νέου αντίστοιχο ενημερωμένο ηλεκτρονικό έγγραφο.

Μετά την επιτυχημένη υποβολή και των δύο εγγράφων, ο χρήστης επισκέπτεται την ΚΔΠ και, αφού αυθεντικοποιηθεί επιτυχώς, αιτείται την παροχή μιας συγκεκριμένης ηλεκτρονικής υπηρεσίας. Η ΚΔΠ μεταφέρει το αίτημα του χρήστη στον ΠΔΙ, ο οποίος αναζητά και ανασύρει την Πολιτική Ιδιωτικότητας της συγκεκριμένης υπηρεσίας και τις προωθεί στο Σημείο Απόφασης (ενέργεια iii Σχήμα 6-4), όπου εκκινεί η διαδικασία σύγκρισής τους (ενέργεια iv Σχήμα 6-4). Στην περίπτωση όπου οι προτιμήσεις δεν αντιτίθενται στην πολιτική ο ΠΔΙ, ενημερώνει τον χρήστη και προωθεί το αίτημά του χρήστη στον αντίστοιχο πάροχο. Σε περίπτωση όπου υπάρχει κάποια διαφορά, ο ΠΔΙ ενημερώνει τον χρήστη επισημαίνοντάς του και τα αντίστοιχα σημεία, σε περίπτωση που επιθυμεί να αναθεωρήσει τις προτιμήσεις του. Σε ένα τυπικό μοντέλο αξιοποίησης πολιτικών και προτιμήσεων ιδιωτικότητας, ο ΠΔΙ θα εκκινούσε μια διαδικασία αμοιβαίας διαπραγμάτευσης μεταξύ του παρόχου και του χρήστη. Ωστόσο, λόγω της νομικής βάσης όλων των υπηρεσιών της Δημόσιας Διοίκησης (ηλεκτρονικών και μη), οι απαιτούμενες αξιώσεις δεν είναι δυνατόν να αλλάξουν και γι' αυτό ζητείται μόνο από τον χρήστη να επανεξετάσεις τις προτιμήσεις του.

6.4 Σενάριο Αξιοποίησης Πολιτικών και Προτιμήσεων Ιδιωτικότητας σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης

Προκειμένου να εξετασθεί η δυνατότητα εφαρμογής των Πολιτικών και των προτιμήσεων Ιδιωτικότητας σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης, αξιοποιήθηκε το μοντέλο της ΚΔΠ που αποτελεί το front end για όλες τις προσφερόμενες ηλεκτρονικές υπηρεσίες. Το σενάριο που επιλέχθηκε, αφορά την ηλεκτρονική υπηρεσία εγγραφής του χρήστη στην Ενιαία Αρχή Πληρωμών του Ελληνικού Δημοσίου που παρέχεται από τη Γενική Γραμματεία Πληροφοριακών Συστημάτων από το 2010. Για την ολοκλήρωση της συγκεκριμένης υπηρεσίας θεωρήθηκε ότι ο χρήστης απαιτείται να έχει λάβει Πιστοποιητικό Φορολογικής Ενημερότητας (ΠΦΕ) από το Υπουργείο Οικονομικών (Ministerial Department of Finance), Πιστοποιητικό Ασφαλιστικής Ενημερότητας (ΠΑΕ) από το Υπουργείο Εργασίας και Κοινωνικών Ασφαλίσεων (Ministerial Department of Insurance) καθώς και έναν έγκυρο Διεθνή Αριθμό Τραπεζικού Λογαριασμού (*IBAN*). Η αντίστοιχη ηλεκτρονική υπηρεσία, με βάση τις απαιτήσεις για παροχή υπηρεσιών μιας στάσης και ύπαρξης διαλειτουργικότητας μεταξύ των παρόχων, θεωρείται ότι δεν απαιτεί από το χρήστη να υποβάλει τα συγκεκριμένα πιστοποιητικά, παρά μόνο να τα αιτηθεί εκ μέρους του. Σύμφωνα με την αρχιτεκτονική που παρουσιάστηκε στην ενότητα 6.3, ο πάροχος κάθε ηλεκτρονικής υπηρεσίας θα πρέπει υποχρεωτικά να υποβάλει την Πολιτική Ιδιωτικότητας για τη συγκεκριμένη υπηρεσία, κατά την αρχική εγγραφή στην ΚΔΠ.

6.4.1 Πολιτικές Ιδιωτικότητας Παρόχων Ηλεκτρονικών Υπηρεσιών

Για τους σκοπούς του συγκεκριμένου σεναρίου, αξιοποιήθηκε ένα απλό σχήμα XML (*XML Schema*) που αποτελείται από συγκεκριμένα elements και attributes, ώστε τόσο οι Πολιτικές όσο και οι Προτιμήσεις Ιδιωτικότητας να περιγραφούν με έναν δομημένο αλλά παράλληλα απλό τρόπο. Εκτός από τα βασικά elements <*Privacy_Policy*> και <*Privacy_Preferences*>, υπάρχουν και τα elements <*Service_Provider*>, <*Electronic_Service*> και <*Description*> προκειμένου να παρέχεται μια συνολικότερη επισκόπηση και περιγραφή της ηλεκτρονικής υπηρεσίας. Στο υπόλοιπο τμήμα του XML εγγράφου γίνεται αναφορά στα δεδομένα του χρήστη που αξιοποιεί η υπηρεσία και αυτά χωρίζονται σε δύο βασικές κατηγορίες: τα προσωπικά αναγνωριστικά και τα προσωπικά δεδομένα. Για καθεμία κατηγορία , προσδιορίζονται συγκεκριμένα elements αναφορικά με την επεξεργασία, την αποθήκευση και την αποστολή σε τρίτους παρόχους. Στον Πίνακας 6-2 παρακάτω παρουσιάζεται η Πολιτική Ιδιωτικότητας για την ηλεκτρονική υπηρεσία “Εγγραφή στην Ενιαία Αρχή Πληρωμών”.

```
<Privacy_Policy>
<Policy_ID="1033">
  <Service_Provider> General Secretary of Information Systems (GSIS)
</Service_Provider>
  <Electronic_Service> Registration at Uniform Payment Authority
</Electronic_Service>
    <Description> Privacy Policy for Registration at Uniform Payment Au-
thority Electronic Service </Description>
</Policy_ID>
<Data>
  <Personal_Identifiers>
    <Identifier_ID="1">National Identity Card Number (IdN)
      <Processed="Confidential">Identification</Proccessed>
      <Storage="Yes" Conserve="90">Payment Order</Storage>
      <Transmitted="Yes">Taxation Awareness Certificate Aquicition
        <Policy_ID="2058"> </Policy_ID>
      </Transmitted>
      <Transmitted="Yes">National Insurance Awareness Certificate Aquici-
tion
        <Policy_ID="3153"> </Policy_ID>
      </Transmitted>
    </Identifier_ID>

    <Identifier_ID="13">Social Security Number (AMKA)
      <Processed="Confidential">Identification</Proccessed>
      <Storage="No"> </Storage>
      <Transmitted="Yes">National Insurance Awareness Certificate Aquici-
tion</Transmitted>
        <Policy_ID="3153"> </Policy_ID>
    </Identifier_ID>

    <Identifier_ID="26">National Taxation Identifier (AFM)
      <Processed="Confidential">Identification</Proccessed>
      <Storage="Yes" Conserve="90">Payment Order</Storage>
      <Transmitted="Yes">Taxation Awareness Certificate Aquicition
</Transmitted>
        <Policy_ID="2058"> </Policy_ID>
    </Identifier_ID>
  </Personal_Identifiers>

  <Personal_Data>
    <Data_ID="321"> IBAN
      <Processed="Confidential">Payment Order</Processed>
      <Storage="Yes" Conserve="90">Payment Order</Storage>
    <Transmitted="No"><Transmitted>
    </Data_ID>

    <Data_ID="32"> First and Last Name
      <Processed="Confidential">Payment Order</Processed>
      <Storage="Yes" Conserve="90">Payment Order</Storage>
           <Transmitted="Yes">Taxation Awareness Certificate Aquicition
        <Policy_ID="2058"> </Policy_ID>
           </Transmitted>
           <Transmitted="Yes">National Insurance Awareness Certificate Aq-
uicition
        <Policy_ID="3153"> </Policy_ID>
      </Transmitted>
    </Data_ID>
  </Personal_Data>
</Data>
</Privacy_Policy>
```

Πίνακας 6-2: Πολιτική Ιδιωτικότητας "Εγγραφή στην Ενιαία Αρχή Πληρωμών"

Το πρώτο τμήμα της Πολιτικής αποτελείται από XML elements, που περιέχουν πληροφορίες για τον πάροχο της υπηρεσίας (*A.3*), την ηλεκτρονική υπηρεσία που αφορά (*A.5*), καθώς και μία συνοπτική περιγραφή της (*A.7 - A.8*). Προκειμένου να διευκολυνθούν οι αναφορές μεταξύ των Πολιτικών, θεωρείται ότι σε καθεμία ανατίθεται από την ΚΔΠ ένας μοναδικός αναγνωριστικός αριθμός (*A.2*). Το συγκεκριμένο αναγνωριστικό αφορά μόνο την συγκεκριμένη ηλεκτρονική υπηρεσία και παραμένει το ίδιο ασχέτως των αναθεωρήσεων που ενδέχεται να πραγματοποιήσει ο πάροχος. Τα δεδομένα που προσδιορίζονται στην συγκεκριμένη πολιτική είναι τρία προσωπικά αναγνωριστικά i) National Identity Card Number (IdN) (*A.10*), ii) Social Security Number (AMKA) (line A.21), iii) National Taxation Identifier (AFM) (*A.28*) και δύο προσωπικά δεδομένα: i) International Bank Account Number (IBAN) number (*A.37*) και το ονοματεπώνυμο του χρήστη (*A.48*). Το *element Identifier_ID* χρησιμοποιείται σε κάθε αναγνωριστικό και περιλαμβάνει ένα attribute με βάση έναν μοναδικό αριθμό που έχει ανατεθεί από την ΚΔΠ σε κάθε προσωπικό αναγνωριστικό, προκειμένου να διευκολυνθούν και πάλι οι αναφορές μεταξύ των παρόχων.

Για το προσωπικό αναγνωριστικό National Identity Card Number (*IdN*) (*A.12*), η πολιτική προσδιορίζει ότι θα το επεξεργαστεί ως εμπιστευτικά δεδομένα (*A.13*), θα το αξιοποιήσει για την ταυτοποίηση του χρήστη και θα το διατηρήσει αποθηκευμένο για 90 ημερολογιακές ημέρες για την έκδοση της εντολής πληρωμής. (*A.14*). Επίσης, θα το προωθήσει στην ηλεκτρονική υπηρεσία National Insurance Awareness Certificate Acquisition, με *policy_ID 2058* (*A.15 – A.16*) και στην ηλεκτρονική υπηρεσία National Insurance Awareness Certificate Acquisition με *policy_ID 3153* (*A.18 - A.20*). Για αυτές τις δύο ηλεκτρονικές υπηρεσίες, η πολιτική δεν περιγράφει πως θα αξιοποιηθεί το συγκεκριμένο αναγνωριστικό καθώς αυτό προσδιορίζεται τις αντίστοιχες πολιτικές ιδιωτικότητας που έχουν υποβάλλει οι πάροχοί τους. Για την ανεύρεση των συγκεκριμένων στοιχείων, ο ΠΔΙ θα πρέπει να τις αναζητήσει στο Αποθετήριο Πολιτικών Ιδιωτικότητας.

Αναφορικά με το Social Security Number (*AMKA*), η πολιτική προσδιορίζει ότι θα τύχει επεξεργασίας σαν εμπιστευτικά δεδομένα για την ταυτοποίηση του χρήστη (*A.25*), δεν θα αποθηκευτεί (A.26) και θα το προωθήσει στην ηλεκτρονική υπηρεσία National Insurance Awareness Certificate Acquisition με *policy_ID 2058* (*A.27-A.29*). Τέλος, το National Taxation Identifier (AFM) θα τύχει επεξεργασίας επίσης σαν εμπιστευτικά δεδομένα, θα αξιοποιηθεί για την ταυτοποίηση του χρήστη (*A.33*), θα διατηρηθεί αποθηκευμένο για 90 ημερολογιακές ημέρες για την έκδοση της εντολής

πληρωμής (*A.34*) και θα προωθηθεί στην ηλεκτρονική υπηρεσία Taxation Awareness Certificate Acquisition με *policy_ID 2058* (*A.35 - A.37*).

Το τελευταίο κομμάτι του εγγράφου αφορά στα προσωπικά δεδομένα του χρήστη που θα αξιοποιήσει η ηλεκτρονική υπηρεσία. Το International Bank Account Number (IBAN) number (line *A.37*) θα τύχει επεξεργασίας σαν εμπιστευτικά δεδομένα και θα χρησιμοποιηθεί για την έκδοση της εντολής πληρωμής (*A.43*), θα αποθηκευθεί για 90 ημερολογιακές ημέρες και δεν θα αποσταλεί σε τρίτο πάροχο. Αντίστοιχα, το ονοματεπώνυμο του χρήστη θα τύχει επεξεργασίας σαν εμπιστευτικά δεδομένα και θα χρησιμοποιηθεί για την έκδοση της εντολής πληρωμής *(A.50*), θα αποθηκευθεί για 90 ημερολογιακές ημέρες και θα προωθηθεί στην ηλεκτρονική υπηρεσία National Insurance Awareness Certificate Acquisition με policy_ID 3153 (*A.54 - A.56*). Οι Πίνακας 6-3 και Πίνακας 6-4, παρακάτω παρουσιάζουν τις Πολιτικές Ιδιωτικότητας για τις ηλεκτρονικές υπηρεσίες Πιστοποιητικό Φορολογικής Ενημερότητας (*National Taxation Awareness Certificate Acquisition*) και Πιστοποιητικό Ασφαλιστικής Ενημερότητας (*National Insurance Awareness Certificate Acquisition*).

```
B.1   <Privacy_Policy>
B.2   <Policy_ID="2058">
B.3           <Service_Provider> Ministerial Department of Finance
B.4   </Service_Provider>
B.5           <Electronic_Service> Taxation Awareness Certificate Aquicition
B.6   </Electronic_Service>
B.7           <Description> Privacy Policy for Taxation Awareness Certificate Aq-
B.8   uicition Electronic Service </Description>
B.9   </Policy_ID>
B.10
B.11  <Data>
B.12          <Personal_Identifiers>
B.13                 <Identifier_ID="1">National Identity Card Number (IdN)
B.14                   <Processed="Confidential">Identification</Proccessed>
B.15                   <Storage="Yes" Conserve="120">Taxation Awareness Certifi-
B.16  cate</Storage>
B.17                   <Transmitted="No">     </Transmitted>
B.18                </Identifier_ID>
B.19
B.20                <Identifier_ID="26">National Taxation Identifier (AFM)
B.21                   <Processed="Confidential"> Identification</Proccessed>
B.22                   <Storage="Yes" Conserve="120">Taxation Awareness Certifi-
B.23  cate</Storage>
B.24                   <Transmitted="No">    </Transmitted>
B.25                 </Identifier_ID>
B.26            </Personal_Identifiers>
B.27
B.28          <Personal_Data>
B.29                <Data_ID="32"> First and Last Name
B.30                   <Processed="Confidential">Taxation Awareness Certifi-
B.31  cate</Processed>
B.32                   <Storage="Yes" Conserve="120"Taxation Awareness Certifi-
B.33  cate</Storage>
B.34                   <Transmitted="No">   <Transmitted>
B.35               </Data_ID>
```

```
B.36            </Personal_Data>
B.37    </Data>
B.38  </Privacy_Policy>
B.39
```

Πίνακας 6-3: Πολιτική Ιδιωτικότητας "Πιστοποιητικό Φορολογικής Ενημερότητας"

Οι Πολιτικές Ιδιωτικότητας των δύο ηλεκτρονικών ακολουθούν την ίδια δομή με την πολιτική που παρουσιάστηκε στον Πίνακας 6-2. Τα πρώτα τμήματα των δύο πολιτικών περιλαμβάνουν XML elements, που περιέχουν το μοναδικό αναγνωριστικό κάθε υπηρεσίας, βασικές πληροφορίες για τον πάροχο, καθώς και μία συνοπτική περιγραφή της υπηρεσίας (*B.2 - B2.9 και Γ.2 – Γ.9*). Στην πολιτική της υπηρεσίας "Πιστοποιητικό Φορολογικής Ενημερότητας", Πίνακας 6-3, δηλώνεται ότι δεδομένα που απαιτούνται είναι το National Identity Card Number (IdN), το National Taxation Identifier (AFM) καθώς και το Ονοματεπώνυμο του χρήστη (*B.13, B.20 και B.30*). Όλα τα δεδομένα θα τύχουν επεξεργασίας ως εμπιστευτικά δεδομένα, θα αξιοποιηθούν για την ταυτοποίηση του χρήστη (*B.14, B.21 & B.30*) και θα αποθηκευθούν για 120 ημερολογιακές ημέρες για την έκδοση του Πιστοποιητικού Φορολογικής Ενημερότητας (*Taxation Awareness Certificate*) (*B.15, B.22 & B.32*). Αντίστοιχα στην πολιτική της υπηρεσίας "Πιστοποιητικό Ασφαλιστικής Ενημερότητας", Πίνακας 6-4 , δηλώνεται ότι δεδομένα που απαιτούνται είναι το National Identity Card Number (*IdN*), το Social Security Number (*AMKA*) και το ονοματεπώνυμο του χρήστη (*Γ.13, Γ.20, Γ.29*). Όλα τα δεδομένα θα τύχουν επεξεργασίας σαν εμπιστευτικά δεδομένα, θα αξιοποιηθούν για την ταυτοποίηση του χρήστη (*Γ.14, Γ.21 & Γ.30*) και θα αποθηκευθούν για 120 ημερολογιακές ημέρες για την έκδοση του Πιστοποιητικού Ασφαλιστικής Ενημερότητας (*Insurance Awareness Certificate*) (*Γ.15, Γ.22 & Γ.32*).

```
Γ.1   <Privacy_Policy>
Γ.2   <Policy_ID="3153">
Γ.3           <Service_Provider> Ministerial Department of National Insurance
Γ.4   </Service_Provider>
Γ.5           <Electronic_Service> National Insurance Awareness Certificate Ac-
Γ.6   quisition </Electronic_Service>
Γ.7           <Description> Privacy Policy for National Insurance Awareness Cer-
Γ.8   tificate Acquisition Electronic Service </Description>
Γ.9   </Policy_ID>
Γ.10
Γ.11  <Data>
Γ.12          <Personal_Identifiers>
Γ.13                 <Identifier_ID="1">National Identity Card Number (IdN)
Γ.14                    <Processed="Confidential">Identification</Proccessed>
Γ.15                    <Storage="Yes" Conserve="30">National Insurance Awareness
Γ.16  Certificate</Storage>
Γ.17                    <Transmitted="No">    </Transmitted>
Γ.18                </Identifier_ID>
Γ.19
Γ.20                <Identifier_ID="23">Social Security Number (AMKA)
Γ.21                    <Processed="Confidential">Identification</Proccessed>
```

```
Γ.22                    <Storage=""Yes" Conserve="30">National Insurance Aware-
Γ.23 ness Certificate</Storage>
Γ.24                    <Transmitted="No">    </Transmitted>
Γ.25                 </Identifier_ID>
Γ.26              </Personal_Identifiers>
Γ.27
Γ.28            <Personal_Data>
Γ.29                  <Data_ID="32"> First and Last Name
Γ.30                    <Processed="Confidential">National Insurance Awareness
Γ.31 Certificate</Processed>
Γ.32                    <Storage=""Yes" Conserve="30">National Insurance Aware-
Γ.33 ness Certificate</Storage>
Γ.34                    <Transmitted="No"> <Transmitted>
Γ.35                </Data_ID>
Γ.36             </Personal_Data>
Γ.37  </Data>
Γ.38 </Privacy_Policy>
Γ.39
```

Πίνακας 6-4: Πολιτική Ιδιωτικότητας "Πιστοποιητικό Ασφαλιστικής Ενημερότητας"

6.4.2 Προτιμήσεις Ιδιωτικότητας Χρήστη

Με βάση την αρχιτεκτονική που προτάθηκε στην ενότητα 6.3, απαιτείται από το χρήστη να υποβάλει τις Προτιμήσεις Ιδιωτικότητάς του στην ΚΔΠ. Στον Πίνακας 6-5 παρουσιάζεται το αντίστοιχο XML έγγραφο για το σενάριο της ενότητας 6.4 Το πρώτο τμήμα των εγγράφου περιλαμβάνει το element, *Preferences_ID*, το οποίο ανατίθεται από την ΚΔΠ σε κάθε έγγραφο και κατά συνέπεια σε κάθε χρήστη. Δεδομένου ότι οι προτιμήσεις ιδιωτικότητας του χρήστη σχετίζονται άμεσα με τον τρόπο που τα προσωπικά δεδομένα του χρήστη θα τύχουν διαχείρισης, κρίνεται αναγκαίο να μην συμπεριλαμβάνεται στο συγκεκριμένο XML καμία πληροφορία για την ψηφιακή ταυτότητα του χρήστη. Στο υπόλοιπο τμήμα του XML εγγράφου γίνεται αναφορά στα δεδομένα του χρήστη που αξιοποιεί η υπηρεσία και χωρίζονται σε δύο βασικές κατηγορίες: τα προσωπικά αναγνωριστικά και τα προσωπικά δεδομένα. Για καθεμία κατηγορία, προσδιορίζονται συγκεκριμένα elements αναφορικά με την επεξεργασία, την αποθήκευση και την αποστολή σε τρίτους παρόχους.

Καθώς μία περιγραφή των προτιμήσεων για κάθε ηλεκτρονική υπηρεσία ξεχωριστά θα ήταν δύσκολο είναι διαχειρίσιμη από το χρήστη, και η περιγραφή ανά πάροχο ενδέχεται να μην επαρκούσε για να αποτυπώσει ο χρήστης τις προτιμήσεις του ανά υπηρεσία προτείνεται η αξιοποίηση συνόλων και υπο-συνόλων, όπως αυτά διαμορφώνονται από κάθε πάροχο και τις ηλεκτρονικές υπηρεσίες που αυτός προσφέρει. Στην περίπτωση που ο χρήστης επιτρέπει την αξιοποίηση των δεδομένων του από έναν συγκεκριμένο πάροχο, θεωρείται ότι επιτρέπει την αξιοποίησή τους και από όλες τις ηλεκτρονικές υπηρεσίες που αυτός προσφέρει. Αντίστοιχα, η έλλειψη αναφοράς ενός συγκεκριμένου παρόχου θεωρείται ως άρνηση αξιοποίησης των δεδομένων του για όλες τις ηλεκτρονικές υ-

πηρεσίες που παρέχει. Με βάση αυτή τη θεώρηση, το απλούστερο έγγραφο XML Προτιμήσεων Ιδιωτικότητας μπορεί να περιλαμβάνει μόνο το element *Preferences_ID* και με βάση την αρχή της άρνησης (P*rinciple of Denial*), κανένας πάροχος και κατά συνέπεια καμία ηλεκτρονική υπηρεσία δεν μπορεί να αξιοποιήσει προσωπικά δεδομένα του συγκεκριμένου χρήστη. Αντίστοιχα, η αξιοποίηση συνόλων και υπερσυνόλων προτείνεται και στον τρόπο αξιοποίησης των προσωπικών δεδομένων. Για παράδειγμα, το attribute *Public* αποτελεί υπερσύνολο του attribute *Confidential*.

```
Δ.1   <Privacy_Preferences>
Δ.2      <Preferences_ID="10451426">     </Preferences_ID>
Δ.3
Δ.4   <Data>
Δ.5
Δ.6        <Personal_Identifiers>
Δ.7           <Identifier_ID="1">National Identity Card Number (IdN)
Δ.8             <Processed="Public">General Secretary of Information Systems
Δ.9   (GSIS)</Proccessed>
Δ.10            <Storage="Yes" Conserve="60">General Secretary of Information Sys-
Δ.11  tems (GSIS)</Storage>
Δ.12            <Processed="Public">Ministerial Department of Finance</Proccessed>
Δ.13            <Storage="Yes" Conserve="60">Ministerial Department of Fi-
Δ.14  nance</Storage>
Δ.15            <Processed="Public">Ministerial Department of National Insur-
Δ.16  ance</Proccessed>
Δ.17            <Storage="Yes" Conserve="60">Ministerial Department of National
Δ.18  Insurance</Storage>
Δ.19          </Identifier_ID>
Δ.20
Δ.21          <Identifier_ID="26">National Taxation Identifier (AFM)
Δ.22            <Processed="Public">General Secretary of Information Systems
Δ.23  (GSIS)</Processed>
Δ.24            <Storage="Yes" Conserve="60">General Secretary of Information Sys-
Δ.25  tems (GSIS)</Storage>
Δ.26            <Processed="Public">Ministerial Department of Finance</Processed>
Δ.27            <Storage="Yes" Conserve="60">Ministerial Department of Fi-
Δ.28  nance</Storage>
Δ.29         </Identifier_ID>
Δ.30
Δ.31         <Identifier_ID="13">Social Security Number (AMKA)
Δ.32           <Processed="Confidential">General Secretary of Information Systems
Δ.33  (GSIS)</Processed>
Δ.34           <Storage="Yes" Conserve="60">General Secretary of Information Sys-
Δ.35  tems (GSIS)</Storage>
Δ.36           <Processed="Confidential">Ministerial Department of National Insur-
Δ.37  ance</Processed>
Δ.38           <Storage="Yes" Conserve="60">Ministerial Department of National
Δ.39  Insurance</Storage>
Δ.40         </Identifier_ID>
Δ.41       </Personal_Identifiers>
Δ.42
Δ.43       <Personal_Data>
Δ.44         <Data_ID="32"> First and Last Name
Δ.45           <Processed="Public">General Secretary of Information Systems
```

```
Δ.46 (GSIS)</Proccessed>
Δ.47          <Storage="Yes" Conserve="360">General Secretary of Information Sys-
Δ.48 tems (GSIS)</Storage>
Δ.49         <Processed="Public">Ministerial Department of Finance</Proccessed>
Δ.50          <Storage="Yes" Conserve="360">Ministerial Department of Fi-
Δ.51 nance</Preserve>
Δ.52         <Processed="Public">Ministerial Department of National Insur-
Δ.53 ance</Proccessed>
Δ.54         <Storage="Yes" Conserve="360">Ministerial Department of National
Δ.55 Insurance</Storage>
Δ.56       </Data_ID>
Δ.57
Δ.58       <Data_ID="321"> IBAN
Δ.59         <Processed="Confidential">General Secretary of Information Systems
Δ.60 (GSIS)</Proccessed>
Δ.61         <Storage="Yes" Conserve="360">General Secretary of Information Sys-
Δ.62 tems (GSIS)</Storage>
Δ.63        </Data_ID>
Δ.64      </Personal_Data>
Δ.65 </Data>
Δ.66 </Privacy_Preferences>
```

Πίνακας 6-5: Προτιμήσεις Ιδιωτικότητας Χρήστη

Στο XML έγγραφο που παρουσιάζεται παραπάνω στον Πίνακας 6-5, ο χρήστης δηλώνει ότι το National Identity Card Number (*IdN*) μπορεί να τύχει επεξεργασίας σαν δημόσιο δεδομένο και να αποθηκευθεί για 60 ημερολογιακές ημέρες από την General Secretary of Information Systems (*GSIS*), το Ministerial Department of Finance και το Ministerial Department of National Insurance (*Δ.8, Δ.12. Δ.15*). Οι ίδιες δηλώσεις ισχύουν και για το Ονοματεπώνυμο του χρήστη με τη μόνο διαφορά ότι μπορούν να αποθηκευθούν για 360 ημερολογιακές ημέρες (*Δ.47, Δ.50, Δ.54*). Για το National Taxation Identifier (*AFM*) ο χρήστης δηλώνει ότι μπορεί να τύχει επεξεργασίας σαν δημόσιο δεδομένο και να αποθηκευθεί για 60 ημερολογιακές ημέρες από το General Secretary of Information Systems (*GSIS*) το Ministerial Department of Finance (*Δ.24, Δ.27*). Το Social Security Number (*AMKA*) μπορεί να τύχει επεξεργασίας μόνο σαν εμπιστευτικό δεδομένο και να αποθηκευθεί για 60 ημερολογιακές ημέρες από το General Secretary of Information Systems (GSIS) και το Ministerial Department of National Insurance (*Δ.32 – Δ.39*). Τέλος, το IBAN μπορεί να τύχει επεξεργασίας μόνο σαν εμπιστευτικό δεδομένο και να αποθηκευθεί για 60 ημερολογιακές ημέρες μόνο από τη General Secretary of Information Systems (*GSIS*) (*Δ.58 – Δ.62*).

6.4.3 Σύγκριση Προτιμήσεων και Πολιτικών Ιδιωτικότητας

Κατά τη διαδικασία σύγκρισης των προτιμήσεων με τις πολιτικές ιδιωτικότητας, ο ΠΔΙ ελέγχει για κάθε τύπο προσωπικών δεδομένων που προσδιορίζεται στις πολιτικές για την ύπαρξη μη συμφωνίας με τις προτιμήσεις του χρήστη. Ο Πίνακας 6-6 παρακάτω, συνοψίζει τα αποτελέσματα της σύγκρισης για το συγκεκριμένο σενάριο. Όπως είναι προφανές εντοπίζονται δύο ασυμφωνίες αναφορικά με τον απαιτούμενο χρόνο διατήρησης – αποθήκευσης των IdN και ΑΦΜ και κατά συνέπεια ο χρήστης θα ενημερωθεί ότι δεν μπορεί να του παρασχεθεί η συγκεκριμένη ηλεκτρονική υπηρεσία.

Προσωπικά Δεδομένα	**Προτιμήσεις Ιδιωτικότητας Χρήστη**				**Πολιτική Ιδιωτικότητας Ηλεκτρονικής Υπηρεσίας**			
	Επεξεργασία	Αποθήκευση	Διατήρηση	Μετάδοση	Επεξεργασία	Αποθήκευση	Διατήρηση	Μετάδοση
IdN	Δημόσιο	Ναι	**60**	Ναι	Εμπιστευτικό	Ναι	**90**	Ναι
ΑΜΚΑ	Εμπιστευτικό	Ναι	60	Ναι	Εμπιστευτικό	Ναι	-	Ναι
ΑΦΜ	Δημόσιο	Ναι	**60**	Ναι	Εμπιστευτικό	Ναι	**90**	Ναι
IBAN	Δημόσιο	Ναι	360	Ναι	Εμπιστευτικό	Ναι	90	Ναι
Όνομα	Δημόσιο	Ναι	360	Ναι	Εμπιστευτικό	Ναι	90	Ναι

Πίνακας 6-6: Σύγκριση Προτιμήσεων και Πολιτικής Ιδιωτικότητας

6.5 Ιεράρχηση Πολιτικών Ιδιωτικότητας

Στα περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης, τα δεδομένα που αξιοποιούνται, είναι διαρθρωμένα σε διαφορετικά επίπεδα, καθώς οι διάφοροι πάροχοι έχουν διαφορετικές ανάγκες τόσο στο είδος όσο και στην επεξεργασία. Αυτές οι ανάγκες μπορεί να διαφέρουν μεταξύ, τους όμως υπόκεινται σε περιορισμούς και υποχρεώσεις που τίθενται από το ισχύων κείμενο νομικό και κανονιστικό πλαίσιο. Από τη σκοπιά της μοντελοποίησης, λοιπόν, η Πολιτική Ιδιωτικότητας κάθε Ηλεκτρονικής Υπηρεσίας τηρεί και ακολουθεί την ακόλουθη ιεραρχία, όπου κάθε βέλος υποδηλώνει ένα μεγαλύτερο επίπεδο γενίκευσης. ***Ηλεκτρονική Υπηρεσία → Πάροχος Ηλεκτρονικής Υπηρεσίας → Υ-***

πουργείο → Δημόσια Διοίκηση. Παρόμοια μοντέλα έχουν προταθεί για τις Προτιμήσεις Ιδιωτικότητας σε Π.Σ. ηλεκτρονικής υγείας (e-Health) (Hong et al., 2007) (Geneiatakis et al., 2009), όμως η εφαρμογή τους δεν έχει εξετασθεί σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης.

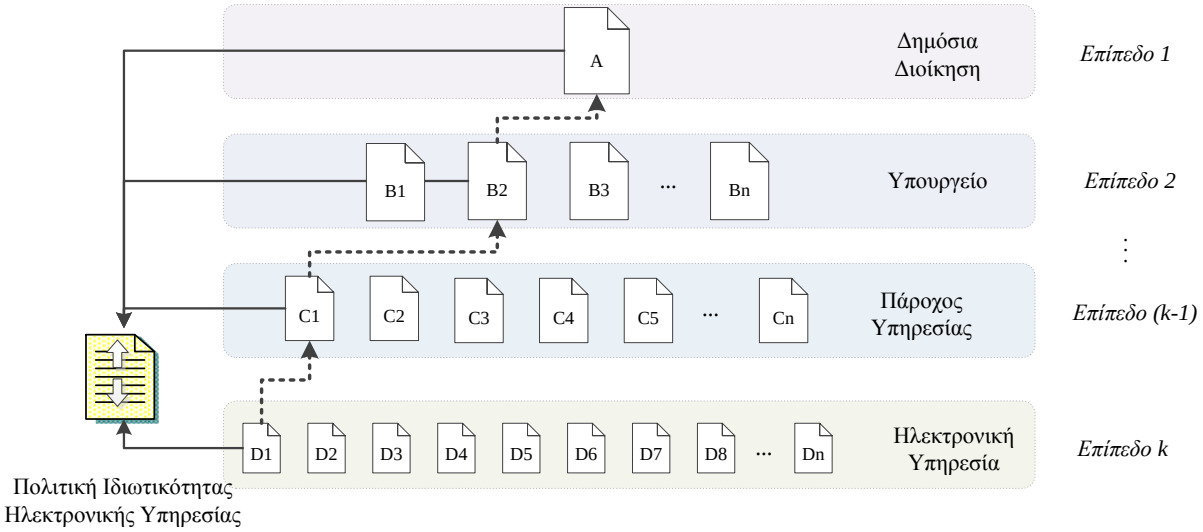
Για μία πιο επίσημη (*formal*) έκφραση του παραπάνω μοντέλου, ορίζεται το P_{CG} ως η Πολιτική Ιδιωτικότητας της Δημόσιας Διοίκησης. το P_{MD} ως η Πολιτική Ιδιωτικότητας ενός Υπουργείου, το P_{SP} ως η Πολιτική Ιδιωτικότητας ενός παρόχου και το P_{ES} ως η Πολιτική Ιδιωτικότητας μια ηλεκτρονικής Υπηρεσίας. Ως εκ τούτου. το P_{ES} μπορεί να θεωρηθεί ως ένα γνήσιο υποσύνολο (proper subset) του P_{SP}, το P_{SP} ως ένα γνήσιο υποσύνολο του P_{MD} και το P_{MD} ως ένα γνήσιο υποσύνολο του P_{CG}, όπως παρουσιάζεται και στην σχέση 6.1 παρακάτω.

$$P_{ES} \subsetneq P_{SP} \subsetneq P_{MD} \subsetneq P_{CG} \tag{6.1}$$

Η αναμενόμενη διάταξη των παραπάνω συνόλων θα ήταν ότι το P_{ES} είναι υποσύνολο (subset) του $P_{SP,}$ το P_{SP} είναι υποσύνολο του P_{MD} και το P_{MD} είναι υποσύνολο του P_{CG}, όμως όσο προχωράμε σε μεγαλύτερο σύνολο (*Superset*), η περιγραφή και οι πληροφορίες που παρέχονται για την αξιοποίηση των δεδομένων αφορούν διαφορετικά επίπεδα abstraction. Για παράδειγμα η P_{CG} περιλαμβάνει περιγραφή σχετικά με το Social Security Number (SSN), το οποίο με βάση το νομικό και κανονιστικό πλαίσιο εντάσσεται, πιθανότατα, στην κατηγορία των προσωπικών αναγνωριστικών και θα πρέπει να αντιμετωπίζεται και να τυγχάνει επεξεργασίας σαν ευαίσθητο – εμπιστευτικό δεδομένο. Η P_{CG} δηλώνει ότι το συγκεκριμένο αναγνωριστικό θα πρέπει όντως να επεξεργάζεται σαν εμπιστευτικά δεδομένα. Στο επόμενο επίπεδο αφαίρεση, η P_{MD} συναινεί υποχρεωτικά σε αυτή την υποχρέωση και προσδιορίζει επιπλέον τους σκοπούς για τους οποίους μπορεί να αξιοποιηθεί, καθώς και το χρονικό διάστημα διατήρησης και αποθήκευσής του. Προχωρώντας σε μικρότερο επίπεδο αφαίρεσης, η P_{SP} σπροσδιορίζει εάν θα επεξεργασθεί και τέλος η P_{ES} εξειδικεύει το σκοπό για την αξιοποίησή του. Προφανώς, ανάλογα με τη δομή στην οποία βασίζεται η Δημόσια Διοίκηση (Ενιαία (*Unitary*), Ομοσπονδιακή (*Federal*) ή Συνομοσπονδιακή (*Con-federal*)) ο αριθμός των συνόλων και των υποσυνόλων ενδέχεται να διαφοροποιείται, όμως μία παρόμοια μοντελοποίηση και αναπαράσταση καθίσταται εφικτή.

Με βάση την αρχιτεκτονική του Πράκτορα Διαχείρισης Ιδιωτικότητας (ΠΔΙ), όπως προτάθηκε στην ενότητα 6.3, όταν η ΚΔΠ λαμβάνει το αίτημα ενός χρήστη για την παροχή μιας συγκεκριμένης ηλεκτρονικής υπηρεσίας, η Πολιτική Ιδιωτικότητας της υπηρεσίας και οι Προτιμήσεις Ιδιωτικότητας του χρήστη, πρέπει να ανακτηθούν και να συγκριθούν για διαφορές (*Conflicts*). Με βάση

την προτεινόμενη ιεραρχία, η Δημόσια Διοίκηση δημιουργεί μία γενική Πολιτική Ιδιωτικότητας, που περιγράφει, σε γενικό επίπεδο, τον τρόπο με τον οποίο συγκεκριμένα προσωπικά δεδομένα και προσωπικά αναγνωριστικά μπορούν να τυγχάνουν επεξεργασίας, να αποθηκεύονται και να αποστέλλονται σε τρίτους παρόχους με βάση το ισχύον νομικό και κανονιστικό πλαίσιο *(Επίπεδο 1)*. Μετακινούμενοι πιο χαμηλά στην ιεραρχία, οι Πολιτικές Ιδιωτικότητας εκδίδονται για συγκεκριμένα Υπουργεία, *(Επίπεδο 2)*, και ακόμα χαμηλότερα για συγκεκριμένες ηλεκτρονικές υπηρεσίες *(Επίπεδο k)*. Σε κάθε ένα από αυτά τα επίπεδα γίνεται αποδοχή όλων των προηγούμενων προσδιορισμών που έχουν πραγματοποιηθεί σε υψηλότερα επίπεδα, μέσω της προσθήκης αναφορών (*References*). Μία σχηματική αναπαράσταση δημιουργίας της Πολιτικής Ιδιωτικότητας για μία ηλεκτρονική υπηρεσία παρουσιάζεται στη συνέχεια στο Σχήμα 6-5.



Σχήμα 6-5: Δημιουργία Πολιτικής Ιδιωτικότητας Ηλεκτρονικής Υπηρεσίας

Ο αριθμός των αναφορών σε προηγούμενα επίπεδα μπορεί να διαφέρει από πολιτική σε πολιτική, δεδομένων των απαιτήσεων και υποχρεώσεων που προσδιορίζει ο πάροχός της και τη δομή της Δημόσιας Διοίκησης. Σε κάθε περίπτωση όμως, όλες οι πολιτικές θα πρέπει να περιέχουν μία έμμεση ή άμεση αναφορά στην Πολιτικής Ιδιωτικότητας *Επιπέδου 1* καθώς έτσι διασφαλίζεται η συμμόρφωση με το ισχύον νομικό και κανονιστικό πλαίσιο.

6.5.1 Κανόνες Ιεραρχικών Πολιτικών Ιδιωτικότητας

Για την διασφάλιση της ομαλής μετάβασης των απαιτήσεων ιδιωτικότητας στα χαμηλότερα επίπεδα της ιεραρχίας, προτείνονται οι ακόλουθοι υποχρεωτικοί κανόνες που θα πρέπει να τηρούνται κατά την εφαρμογή των ιεραρχικών πολιτικών.

Κανόνας 1: Κάθε μία από τις Πολιτικές Ιδιωτικότητας {*Επίπεδο(k), Επίπεδο (k-1), ⋯ , Επίπεδο 3, Επίπεδο 2*} πρέπει να συμμορφώνεται με την Πολιτική Ιδιωτικότητας Επιπέδου 1.

Η συμμόρφωση μιας Πολιτικής Ιδιωτικότητας Ηλεκτρονικής Υπηρεσίας ορίζεται ως η απουσία άρνησης ή γενίκευσης των διατάξεων και των υποχρεώσεων που επιβάλλει.

Κανόνας 2: Κάθε μία από τις Πολιτικές Ιδιωτικότητας {*Επίπεδο(k), Επίπεδο (k-1), ⋯ , Επίπεδο 3, Επίπεδο 2*} πρέπει να περιέχει έμμεση ή άμεση αναφορά στην Πολιτική Ιδιωτικότητας Επιπέδου 1.

Κανόνας 3: Κάθε μία από τις Πολιτικές Ιδιωτικότητας {*Επίπεδο(k), Επίπεδο (k-1), ⋯ , Επίπεδο 3, Επίπεδο 2*} μπορεί να εισάγει καινούργιες διατάξεις ή υποχρεώσεις, με την προϋπόθεση να μην έρχονται σε αντίθεση με αυτές που επιβάλλονται από Πολιτικές Ιδιωτικότητας προηγούμενων επιπέδων.

Κανόνας 4: Κάθε μία από τις Πολιτικές Ιδιωτικότητας {*Επίπεδο(k), Επίπεδο (k-1), ⋯ , Επίπεδο 3, Επίπεδο 2*} μπορεί μόνο να συγκεκριμενοποιεί και να εξειδικεύει διατάξεις και υποχρεώσεις που επιβάλλονται από Πολιτικές Ιδιωτικότητας προηγούμενων επιπέδων.

Συγκεκριμενοποίηση των διατάξεων (S) και των υποχρεώσεων (C) επιτρέπεται μόνο όταν οι καινούργιες διατάξεις (S') και υποχρεώσεις (C') είναι υποσύνολο των S και C αντίστοιχα.

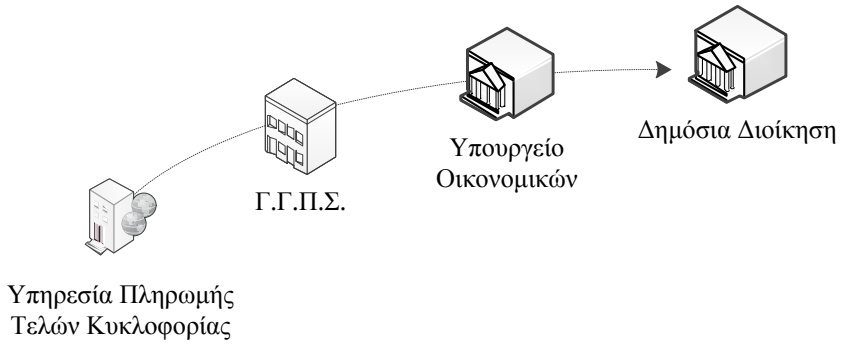
Η ανάπτυξη της προτεινόμενης προσέγγισης προωθεί τη διαλειτουργικότητα των ηλεκτρονικών υπηρεσιών και τη συμμόρφωσή τους με το ισχύον νομικό και κανονιστικό πλαίσιο. Κάτι τέτοιο, μπορεί να θεωρηθεί όχι μόνο σαν ελεγκτικός μηχανισμός αλλά και σαν διαδικασία άμεσης εναρμόνισης σε ενδεχόμενο τροποποίηση του υποκείμενου νομικό και κανονιστικό πλαίσιο. Μια νεοεισα-

χθείσα νομοθετική ή κανονιστικό αλλαγή θα απαιτούσε την ενσωμάτωσή της σε κάθε πολιτική ξεχωριστά. Επιπλέον, τα παραγόμενα XML έγγραφα έχουν σημαντικά μικρότερο μέγεθος λόγω της μη-επανάληψης των πληροφορικών Τέλος, μπορεί να εφαρμοστεί και σε ομόσπονδα περιβάλλοντα ή σε παροχή διακρατικών υπηρεσιών Ηλεκτρονικής Διακυβέρνησης όπως προτείνεται και στην απόφαση 2004/387/ΕΚ με τίτλο "*περί της διαλειτουργικής παροχής πανευρωπαϊκών υπηρεσιών ηλεκτρονικής διακυβέρνησης στις δημόσιες διοικήσεις. τις επιχειρήσεις και τους πολίτες (IDABC)*".

Το μειονέκτημα της συγκεκριμένης μεθοδολογίας είναι το επιπρόσθετο υπολογιστικό κόστος που εισάγεται στον ΠΔΙ καθώς για κάθε αίτηση παροχής υπηρεσίας απαιτείται να αναζητήσει όλες τις πολιτικές στις οποίες γίνεται αναφορά. Όμοια όμως με τις ιεραρχίες σε Υποδομές Δημοσίου Κλειδιού (Henderson et al., 2002), (Lambrinoudakis et al., 2003), (Zhao & Smith, 2006), (Satizábal et al., 2006) ο ΠΔΙ μπορεί να μειώσει τις συγκεκριμένες αναζητήσεις διατηρώντας τοπικά συγκεκριμένες ιεραρχικές πολιτικές και ανανεώνοντάς τες ανά τακτά χρονικά διαστήματα.

6.5.2 Σενάριο Αξιοποίησης Ιεραρχικών Πολιτικών Ιδιωτικότητας

Προκειμένου να εξετασθεί η δυνατότητα εφαρμογής των ιεραρχικών Πολιτικών Ιδιωτικότητας σε σύγχρονα Π.Σ. αξιοποιήθηκε το μοντέλο της ΚΔΠ που αποτελεί το front end για όλες τις προσφερόμενες ηλεκτρονικές υπηρεσίες και παράλληλα ενσωματώνει και τον ΠΔΙ. Το σενάριο που επιλέχθηκε αφορά την ηλεκτρονική υπηρεσία πληρωμής τελών κυκλοφορίας (Annual Vehicle Tax) που θεωρήθηκε ότι προσφέρεται από τη Γενική Γραμματεία Πληροφοριακών Συστημάτων (*General Secretary of Information Systems (GSIS)*) η οποία λειτουργεί κάτω από την εποπτεία του Υπουργείου Οικονομικών (*Ministerial Department of Finance*). Η ιεραρχία της συγκεκριμένης υπηρεσίες παρουσιάζεται παρακάτω στο Σχήμα 6-6. Για την επιτυχή ολοκλήρωση της συγκεκριμένης υπηρεσίας ο χρήστης πρέπει να υποβάλλει το National Taxation Number (AFM) καθώς και τον αριθμό κυκλοφορίας του οχήματος (*Vehicle's license plate*). Η GSIS επαληθεύει την εγκυρότητα των δεδομένων και δημιουργεί ένα έγγραφο πληρωμής που περιλαμβάνει το ονοματεπώνυμο του χρήστη, τον αριθμό κυκλοφορίας του οχήματος, το συνολικό κόστος του τέλους κυκλοφορίας καθώς και ένα μοναδικό αριθμό πληρωμής (*Unique payment identifier*) που θα χρησιμοποιηθεί από το χρηματοπιστωτικό ίδρυμα το οποίο θα πραγματοποιηθεί η πληρωμή.



Σχήμα 6-6: Ιεραρχία Ηλεκτρονικής Υπηρεσίας

Όμοια με την ενότητα 6.4, για τους σκοπούς του συγκεκριμένου σεναρίου, αξιοποιήθηκε ένα απλό σχήμα XML (*XML Schema*) που αποτελείται από συγκεκριμένα elements και attributes ώστε οι Πολιτικές Ιδιωτικότητας να περιγραφούν με έναν δομημένο αλλά παράλληλα απλό τρόπο. Κάθε έγγραφο XML περιλαμβάνει ένα *Privacy_Policy* element, ένα *Policy_ID* element, στο οποίο αναφέρεται το μοναδικό αναγνωριστικό κάθε πολιτικής όπως ανατίθεται από την ΚΔΠ, και ένα *Data* element. Το τελευταίο χωρίζεται σε δύο sub-elements, *Personal_Identifiers* and *Personal_Data* ανάλογα με τον τύπο των δεδομένων που θα περιγραφούν

Η Πολιτική Ιδιωτικότητας της Δημόσιας Διοίκησης που παρουσιάζεται στον Πίνακας 6-7 παρακάτω δηλώνει ότι το *National Taxation Identifier (E.7),* το *License Plate (E.1)* καθώς και το Ονοματεπώνυμο του χρήστη *(E.19)* θα πρέπει να επεξεργάζονται σαν εμπιστευτικά δεδομένα και μπορούν να αποθηκεύονται από τους παρόχους ηλεκτρονικών υπηρεσιών και να αποστέλλονται σε τρίτους παρόχους. Δεν γίνεται καμία αναφορά στην αιτία της επεξεργασίας όπως και στο χρονικό διάστημα της αποθήκευσης και ως εκ τούτου θα πρέπει να προσδιορίζονται και να συγκεκριμενοποιούνται από πολιτικές χαμηλότερου επιπέδου ιεραρχίας. Όσο αφηρημένη και να φαίνεται η συγκεκριμένη πολιτική, αυτές είναι οι βασικοί περιορισμοί και υποχρεώσεις που όλα τα Υπουργεία και τους παρόχους ηλεκτρονικών υπηρεσιών.

```
 E.1  <Privacy_Policy>
 E.2   <Policy_ID="001">
 E.3  <Description> Hellenic Government Privacy Policy  </Description>
 E.4  </Policy_ID>
 E.5  <Data>
 E.6    <Personal_Identifiers>
 E.7      <Identifier_ID="26"> National Taxation Identifier (AFM)
 E.8        <Processed="Confidential">  </Proccessed>
 E.9        <Storage="Yes"> </Storage>
E.10          <Transmitted="Yes" </Transmitted>
E.11      </Identifier_ID>
```

```
E.12    </Personal_Identifiers>
E.13    <Personal_Data>
E.14      <Data_ID="873"> License Plate
E.15        <Processed="Confidential"> </Processed>
E.16        <Storage="Yes"> </Storage>
E.17          <Transmitted="Yes" </Transmitted>
E.18      </Data_ID>
E.19      <Data_ID="32"> First and Last Name
E.20        <Processed="Confidential">  </Processed>
E.21        <Storage="Yes"> </Storage>
E.22          <Transmitted="Yes" </Transmitted>
E.23      </Data_ID>
E.24    </Personal_Data>
E.25  </Data>
E.26  </Privacy_Policy>
```

Πίνακας 6-7: Πολιτική Ιδιωτικότητας Δημόσιας Διοίκησης

Στην πολιτική Ιδιωτικότητας του Υπουργείου Οικονομικών που παρουσιάζεται στον Πίνακας 6-8 παρακάτω, το attribute *P_Ref_ID* εισάγεται για να υποδηλώνει την αναφορά σε έγγραφο πολιτικής XML υψηλότερου επιπέδου. Συγκεκριμένα, στις γραμμές *Z.7*, *Z.13* και *Z.17* γίνεται αναφορά στο XML έγγραφο με *P_Ref_ID="001"* στο οποίο αντιστοιχεί η Πολιτική Ιδιωτικότητας της Δημόσιας Διοίκησης. Μέσω των συγκεκριμένων αναφορών ενσωματώνονται στην παρούσα πολιτική οι περιγραφές των δεδομένων που έχουν προηγηθεί στην πολιτική της Δημόσιας Διοίκησης και πλέον είναι αναγκαία μόνο η συγκεκριμενοποίησή τους. Στη γραμμή *Z.8* δηλώνεται ότι το National Taxation Identifier θα αξιοποιηθεί για την ταυτοποίηση του χρήστη, στις γραμμές Z.9 και Z.15 ότι τα αντίστοιχα δεδομένα μπορούν να αποθηκευθούν για 365 ημερολογιακές ημέρες και στη γραμμή Z.19 ότι το ονοματεπώνυμο του χρήστη μπορεί να αποθηκευθεί για 90 ημερολογιακές ημέρες. Η έλλειψη του element <*Transmitted*> υποδηλώνει ότι η περιγραφή που υπάρχει στην αναφερόμενη πολιτική με *ID 001* παραμένει σε ισχύ.

```
Z.1   <Privacy_Policy>
Z.2    <Policy_ID="024">
Z.3   <Description> Ministry of Finance Privacy Policy </Description>
Z.4   </Policy_ID>
Z.5   <Data>
Z.6     <Personal_Identifiers>
Z.7       <Identifier_ID="26" P_Ref_ID="001"> National Taxation Identifier
Z.8   (AFM)
Z.9         <Processed="Confidential"> Identification </Proccessed>
Z.10        <Storage="Yes" Retention="365"> </Storage>
Z.11      </Identifier_ID>
Z.12    </Personal_Identifiers>
Z.13    <Personal_Data>
Z.14      <Data_ID="873" P_Ref_ID ="001"> License Plate
Z.15        <Processed="Confidential"> </Processed>
Z.16        <Storage="Yes" Retention ="365"> </Storage>
Z.17      </Data_ID>
Z.18      <Data_ID="32" p_Ref_ID="001"> First and Last Name
Z.19        <Processed="Confidential"> </Processed>
```

```
Z.20        <Storage="Yes" Retention="90"> </Storage>
Z.21      </Data_ID>
Z.22    </Personal_Data>
Z.23  </Data>
Z.24  </Privacy_Policy>
```

Πίνακας 6-8: Πολιτική Ιδιωτικότητας Υπουργείου Οικονομικών

Ο Πίνακας 6-9 στη συνέχεια, παρουσιάζει την Πολιτική Ιδιωτικότητας της Γ.Γ.Π.Σ.. όπου πάλι γίνεται αναφορά στο XML έγγραφο με *P_Ref_ID="024"* (*Η.7, Η.12 και Η.13*). Η συγκεκριμένη πολιτική ανήκει στο Υπουργείο Οικονομικών. Η μόνη διαφοροποίηση έγκειται στον προσδιορισμό του χρόνου αποθήκευσης του National Taxation Identifier που μειώνεται στις 180 ημερολογιακές ημέρες. (*Η.8*). Η συγκεκριμένη αλλαγή μπορεί να πραγματοποιηθεί, καθώς αποτελεί εξειδίκευση της περιγραφής που υπήρχε στην υψηλότερου επιπέδου πολιτική του Υπουργείου Οικονομικών.

```
H.1   <Privacy_Policy>
H.2    <Policy_ID="587">
H.3   <Description> GSIS Privacy Policy </Description>
H.4    </Policy_ID>
H.5    <Data>
H.6     <Personal_Identifiers>
H.7       <Identifier_ID="26" P_Ref_ID="024"> National Taxation Identifier
H.8   (AFM)
H.9           <Storage="Yes" Retention="180"></Storage>
H.10      </Identifier_ID>
H.11    </Personal_Identifiers>
H.12     <Personal_Data>
H.13      <Data_ID="873" P_Ref_ID ="024"> License Plate </Data_ID>
H.14      <Data_ID="32" p_Ref_ID="024"> First and Last Name </Data_ID>
H.15
H.16    </Personal_Data>
H.17   </Data>
H.18  </Privacy_Policy>
```

Πίνακας 6-9: Πολιτική Ιδιωτικότητας Γ.Γ.Π.Σ.

Η τελευταία Πολιτική Ιδιωτικότητας αφορά την ηλεκτρονική υπηρεσία για την έκδοση πληρωμής των τελών κυκλοφορίας και παρουσιάζεται στον Πίνακας 6-10 παρακάτω. Σε σχέση με τα XML έγγραφα πολιτικών που παρουσιάστηκαν προηγουμένως, η συγκεκριμένη περιλαμβάνει και τα elements <*Service_Provider*> και <*Electronic_Service*> (*Θ.3 και Θ.5*), καθώς αφορά μία παρεχόμενη ηλεκτρονική υπηρεσία και πρέπει να είναι εμφανείς, ο πάροχος και ο σκοπός της. Στις γραμμές *Θ.12, Θ.18* και *Θ.24* γίνεται αναφορά στην πολιτική με *P_Ref_ID="587"* και οι μοναδικές αλλαγές εντοπίζονται στην άρνηση αποστολής του National Taxation Identifier (AFM) σε τρίτο πάροχο

(*Θ.14)*, στην αξιοποίηση του License Plate για την ταυτοποίηση του χρήστη (Θ.19), την αποθήκευσή του για 90 ημερολογιακές ημέρες (*Θ.21*), την αξιοποίηση του ονοματεπώνυμου του χρήστη για την ταυτοποίησή του (*Θ.25*) και την άρνηση αποστολής και διατήρησής του *(Θ.27).*

```
Θ.1  <Privacy_Policy>
Θ.2   <Policy_ID="1038">
Θ.3  <Service_Provider> General Secretary of Information Systems (GSIS)
Θ.4  </Service_Provider>
Θ.5    <Electronic_Service> Annual Vehicle Tax </Electronic_Service>
Θ.6  <Description> Privacy Policy for Annual Vehicle Tax Electronic Ser-
Θ.7  vice  </Description>
Θ.8  </Policy_ID>
Θ.9  <Data>
Θ.10   <Personal_Identifiers>
Θ.11     <Identifier_ID="26" P_Ref_ID="587"> National Taxation Identifier
Θ.12 (AFM)
Θ.13           <Transmitted="No" </Transmitted>
Θ.14     </Identifier_ID>
Θ.15   </Personal_Identifiers>
Θ.16   <Personal_Data>
Θ.17     <Data_ID="873" P_Ref_ID ="587"> License Plate
Θ.18         <Processed="Confidential"> Identification </Proccessed>
Θ.19        <Storage="Yes" Retention="90"> </Storage>
Θ.20      </Data_ID>
Θ.21 <Transmitted=”Yes” </Transmitted>
Θ.22     <Data_ID="32" p_Ref_ID="587"> First and Last Name
Θ.23        <Processed="Confidential"> Identification </Proccessed>
Θ.24      <Storage="No" Retention="0"> </Storage>
Θ.25      </Data_ID>
Θ.26   </Personal_Data>
Θ.27 </Data>
Θ.28 </Privacy_Policy>
```

Πίνακας 6-10: Πολιτική Ιδιωτικότητας Ηλεκτρονικής Υπηρεσίας “Τέλη Κυκλοφορίας”

6.5.3 Σύνθεση Πολιτικής Ιδιωτικότητας Τελικής Υπηρεσίας

Για την παροχή της τελικής υπηρεσίας, ο ΠΔΙ θα πρέπει να συνθέσει την τελική πολιτική με βάση τις αναφορές που περιλαμβάνει κάθε XML έγγραφο. Ο Πίνακας 6-11 παρακάτω παρουσιάζει συγκεντρωτικά τις περιγραφές και τις υποχρεώσεις όλων των οντοτήτων που συμμετέχουν στην συγκεκριμένη ιεραρχία. Μία παρόμοια γραφική αναπαράσταση θα μπορούσε να αξιοποιηθεί από τον ΠΔΙ για εύκολο και αποδοτικό έλεγχο συμμόρφωσης όλων των ιεραρχικών Πολιτικών Ιδιωτικότητας.

	AVT					*GSIS*					*Υπουργείο Οικονομικών*					*Δημόσια Διοίκηση*				
	Storage	*Process*	*Purpose*	*Retention*	*Transmit*	*Storage*	*Process*	*Purpose*	*Retention*	*Transmit*	*Storage*	*Process*	*Purpose*	*Retention*	*Transmit*	*Storage*	*Process*	*Purpose*	*Retention*	*Transmit*
ΑΦΜ	►	►	►	►	Όχι	►	►	►	180	►	►	►	*T*	365	►	Ναι	*E*	◄	◄	Ναι
Αριθμός Πινακίδας	►	►	*T*	90	►	►	►	◄	►	►	►	►	◄	365	►	Ναι	*E*	◄	◄	Ναι
Ον/μο	Όχι	►	*T*	►	►	►	►	◄	►	►	►	►	◄	90	►	Ναι	*E*	◄	◄	Ναι

T : Ταυτοποίηση *E: Εμπιστευτικά*

►*: Αναφέρεται σε πολιτική υψηλότερου επιπέδου* ◄*: Αναφέρεται σε πολιτική χαμηλότερου επιπέδου*

Πίνακας 6-11: Σύνοψη Σύνθεσης Πολιτικής Ιδιωτικότητας Τελικής Υπηρεσίας

6.5.4 Σύγκριση με Μη-Ιεραρχικές Πολιτικές Ιδιωτικότητας

Ένα άμεσα αναγνωρίσιμο πλεονέκτημα των ιεραρχικών Πολιτικών Ιδιωτικότητας είναι η μείωση του μεγέθους των παραγόμενων Πολιτικών Ιδιωτικότητας, εκτός από τη συμμόρφωση με το ισχύον νομικό και κανονιστικό πλαίσιο. Στο πλαίσιο του σεναρίου αξιοποίησης, στην ενότητα 6.5.2, μόνο η Πολιτική Ιδιωτικότητας της Ηλεκτρονικής Υπηρεσίας "Τέλη Κυκλοφορίας" θα αποτελούνταν από επιπλέον 100 χαρακτήρες ASCII, όπως παρουσιάζεται στον Πίνακας 6-12. Όσο ασήμαντη και να διαφαίνεται αυτή η μείωση, όταν εφαρμοστεί, κατ' αναλογία, σε όλα XML έγγραφα τον Υπουργείων, παρόχων και ηλεκτρονικών υπηρεσιών, μπορεί να οδηγήσει σε σημαντική μείωση του όγκου μεταδιδόμενης, αποθηκευμένης και επεξεργάσιμης πληροφορίας.

```
 I.1   <Privacy_Policy>
 I.2    <Policy_ID="1038">
 I.3   <Service_Provider> General Secretary of Information Systems
 I.4   (GSIS) </Service_Provider>
 I.5     <Electronic_Service> Annual Vehicle Tax
 I.6   </Electronic_Service>
 I.7   <Description> Privacy Policy for Annual Vehicle Tax Elec-
 I.8   tronic Service  </Description>
 I.9   </Policy_ID>
I.10   <Data>
I.11     <Personal_Identifiers>
I.12       <Identifier_ID="26"> National Taxation Identifier (AFM)
I.13           <Processed="Confidential"> Identification
I.14   </Proccessed>
I.15          <Storage="Yes" Retention="90"> </Storage>
```

```
I.16          <Transmitted="Yes" </Transmitted>
I.17       </Identifier_ID>
I.18     </Personal_Identifiers>
I.19     <Personal_Data>
I.20       <Data_ID="873"> License Plate
I.21           <Processed="Confidential"> Identification
I.22  </Proccessed>
I.23          <Storage="Yes" Retention="90"> </Storage>
I.24           <Transmitted="Yes" </Transmitted>
I.25       </Data_ID>
I.26  <Transmitted=”Yes” </Transmitted>
I.27      <Data_ID="32"> First and Last Name
I.28         <Processed="Confidential"> Identification
I.29  </Proccessed>
I.30       <Storage="No" Retention="0"> </Storage>
I.31       </Data_ID>
I.32    </Personal_Data>
I.33  </Data>
I.34  </Privacy_Policy>
```

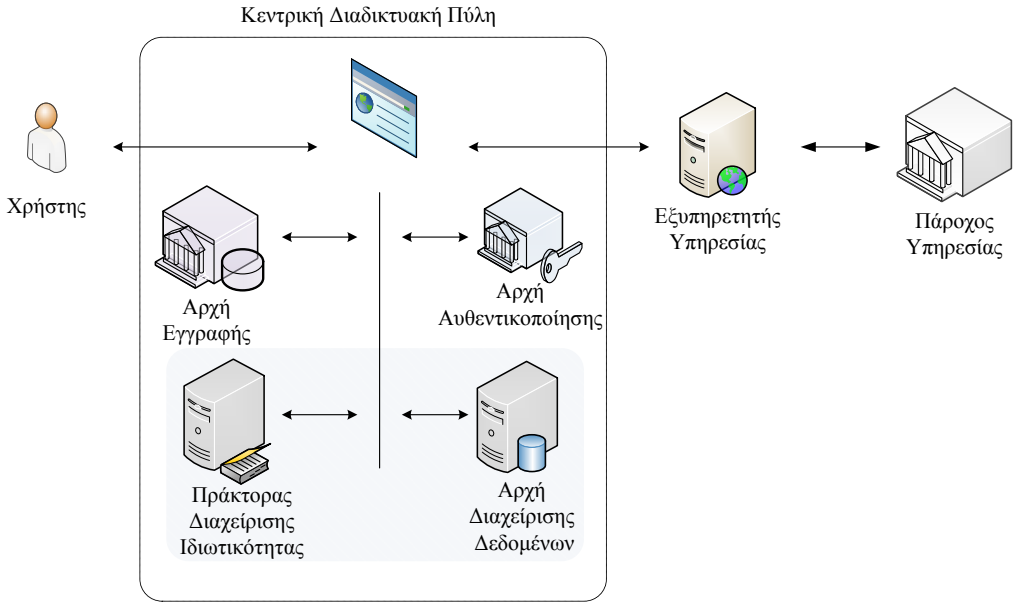
Πίνακας 6-12: Μη Ιεραρχική Πολιτική Ιδιωτικότητας Ηλεκτρονικής Υπηρεσίας "Τέλη Κυκλοφορίας"

6.6 Διαχείριση Προσωπικών Δεδομένων Χρηστών

Το σκεπτικό της ασφαλούς διαχείρισης προσωπικών δεδομένων στο Διαδίκτυο και η αξιοποίησή της από ηλεκτρονικές υπηρεσίες έχει προταθεί σε ερευνητικό επίπεδο για Πληροφοριακά Συστήματα Ηλεκτρονικού Εμπορίου (*e-Commerce*) (Bertino et al., 2002) (Bertino et al., 2004) (Carminati & Ferrari, 2005) (Efraimidis et al., 2008). Η υλοποίηση των συγκεκριμένων προτάσεων βασίζεται στην ύπαρξη δεσμευτικών συμβολαίων ιδιωτικότητας (*Privacy Contracts*) μεταξύ του υποκειμένου των δεδομένων (*Data Subject*) και του παρόχου (*Data Consumer*), καθώς και στην ύπαρξη μιας οντότητας που θα είναι υπεύθυνη για την αποθήκευση και διάθεσή τους μόνο όταν ικανοποιούνται οι απαιτήσεις των συμβολαίων.

Με βάση το μοντέλο των σύγχρονων Π.Σ. Ηλεκτρονικής Διακυβέρνησης που υλοποιούν μία Κεντρική Διαδικτυακή πύλη, σαν το front end όλων των ηλεκτρονικά παρεχόμενων υπηρεσιών, την ενσωμάτωση την Αρχών Εγγραφής και Αυθεντικοποίησηςγια παροχή υπηρεσιών μιας στάσης, καθώς και την πρόταση αξιοποίησης Πολιτικών και Προτιμήσεων Ιδιωτικότητας, όπως περιγράφεται στην ενότητα 6.2.2, εξετάζεται η δυνατότητα διαχείρισης προσωπικών δεδομένων των χρηστών. Η αρχιτεκτονική που παρουσιάζεται στο Σχήμα 6-7 στη συνέχεια, επιτρέπει την ασφαλή αποθήκευση και διαχείριση των προσωπικών δεδομένων των χρηστών, με βάση τις πολιτικές και τις προτιμήσεις που έχουν υποβληθεί στον Πράκτορα Διαχείρισης Ιδιωτικότητας. Μετά την επιτυχή υποβολή των Προτιμήσεων Ιδιωτικότητάς του, ο χρήστης αποστέλλει τα προσωπικά δεδομένα που επιθυμεί, στην

Αρχή Διαχείρισης Δεδομένων (*ΑΔΔ*). Το συγκεκριμένο τμήμα της ΚΔΠ είναι υπεύθυνο για την αποθήκευση των δεδομένων που υποβάλλει κάθε χρήστης, και την αποστολή τους στον αντίστοιχο πάροχο για την ολοκλήρωσης μιας ηλεκτρονικής υπηρεσίας.



Σχήμα 6-7: Αρχιτεκτονική Διαχείρισης Προσωπικών Δεδομένων σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης

Ο χρήστης αιτείται την παροχή μιας ηλεκτρονικής υπηρεσίας στην ΚΔΠ και ο ΠΔΙ ελέγχει τη συμμόρφωση των Προτιμήσεων Ιδιωτικότητάς του με την Πολιτική Ιδιωτικότητας της συγκεκριμένης υπηρεσίας. Σε περίπτωση που δεν υπάρχει κάποια διένεξη, ενημερώνεται ο χρήστης και μεταβιβάζεται το αίτημά του στην ΑΔΔ, για αποστολή των κατάλληλων προσωπικών δεδομένων στον πάροχο της υπηρεσίας. Προκειμένου να διασφαλιστεί η ιδιωτικότητά και η ακεραιότητά τους κατά τη μεταφορά, η ΑΔΔ, αξιοποιώντας την υποδομή Δημοσίου Κλειδιού της Δημόσιας Διοίκησης, κρυπτογραφεί τα δεδομένα με το Δημόσιο Κλειδί του παρόχου, τα υπογράφει ψηφιακά και τα αποστέλλει. Ο πάροχος της υπηρεσίας λαμβάνει πλέον τόσο το αίτημα του χρήστη όσο και τα δεδομένα που απαιτούνται για την ολοκλήρωσή του.

Ανεξάρτητα από το πόσο δελεαστική και υποσχόμενη είναι η προοπτική της ασφαλούς διαχείρισης προσωπικών δεδομένων από την ΚΔΠ, η φύση τους επιβάλλει την ανάγκη διασφάλισης συγκεκριμένου επιπέδου ασφάλειας και ιδιωτικότητας με σκοπό να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση από τρίτους και η κατάχρησή τους. Αντίστοιχα, θα πρέπει να εξετασθεί και το ισχύον νο-

μικό και κανονιστικό πλαίσιο αναφορικά με το ποια προσωπικά δεδομένα και σε ποιο βαθμό είναι θεμιτό και επιτρεπτό να αποθηκεύονται.

ΚΕΦΑΛΑΙΟ 7 - ΣΥΜΠΕΡΑΣΜΑΤΑ

Στο παρόν κεφάλαιο επιχειρείται μια συνολική αποτίμηση της παρούσας διατριβής. Συνοψίζονται τα ερευνητικά αποτελέσματα και αποτυπώνονται δύο βασικές κατευθύνσεις για περαιτέρω έρευνα στην ευρύτερη περιοχή της ασφάλειας και προάσπισης της ιδιωτικότητας σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης.

7.1 Συμπεράσματα

Η Ηλεκτρονική Διακυβέρνηση παρέχει πολλαπλές και ποικιλόμορφες ευκαιρίες για τη Δημόσια Διοίκηση, μέσω της χρήσης και αξιοποίησης σύγχρονων τεχνολογιών και μεθοδολογιών, προς την κατεύθυνση του ανασχεδιασμού των διοικητικών διαδικασιών, την αναδιοργάνωση, τη βελτίωση λειτουργίας και τον έλεγχο των παρεχόμενων υπηρεσιών, την παροχή καινούργιων διαδικασιών πρόσβασης και διάχυσης της απαραίτητης πληροφορίας, καθώς και της συνολικής σχέσης μεταξύ Δημόσιας Διοίκησης και πολιτών. Για να καταστεί όμως δυνατή και επιτυχημένη μία τέτοια μετάβαση δεν αρκεί η αυτοματοποίηση των υπαρχουσών διαδικασιών και η παροχή τους μέσω του Διαδικτύου ή η αυτούσια μεταφορά ενός γραφειοκρατικού συστήματος σε ηλεκτρονική μορφή. Απαιτείται ένας ολιστικός ανασχεδιασμός της Δημοσίας Διοίκησης ώστε αυτή να καταστεί πραγματικά ανοιχτή (*Open*), συνεργατική (*Collaborative*) και διαλειτουργική (*Interoperable*), παύοντας πλέον να λειτουργεί στα στενά όρια ενός τμήματος ή μεμονωμένα μιας Δημοσίας Υπηρεσίας, παράλληλα με την αξιοποίηση και την ενσωμάτωση καινούργιων καινοτόμων τεχνολογιών.

Η Δημόσια Διοίκηση καλείται να εγκαθιδρύσει και να διατηρήσει καθολικά ένα επίπεδο προστασίας, ασφάλειας και εμπιστοσύνης, όχι μόνο αντίστοιχο και ισότιμο με αυτό των υπαρχόντων υπηρεσιών αλλά ικανό να διασφαλίσει ότι τα προσωπικά δεδομένα αξιοποιούνται με τρόπο διαφανή και σύννομο λαμβάνοντας υπ' όψιν το συμφέρον των πολιτών. Η αξιοποίηση και ενσωμάτωση των ΤΠΕ, εισάγει καινούργιες απειλές που απαιτούν τη μελέτη και εφαρμογή μηχανισμών και μεθοδολογιών ασφάλειας, ικανών να εγγυηθούν την αυθεντικότητα της ψηφιακής ταυτότητας των συναλλασσόμενων, την ακεραιότητα και την εμπιστευτικότητα του περιεχομένου κάθε συναλλαγής καθώς και τη μη-αποποίηση συμμετοχής και ολοκλήρωσης της συναλλαγής.

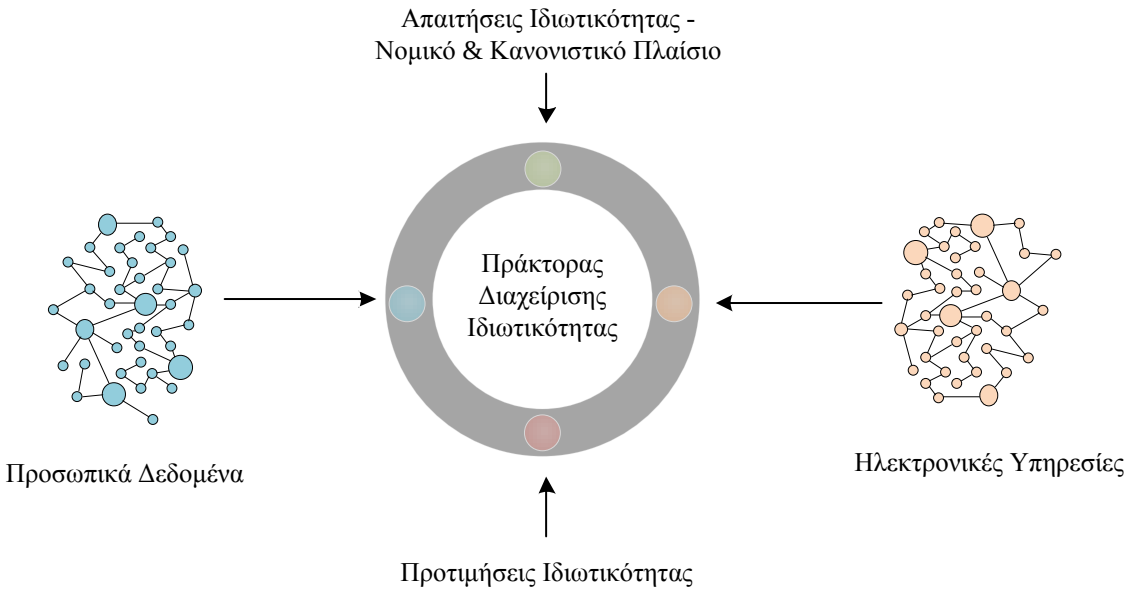
Σκοπός της παρούσας διατριβής ήταν η μελέτη εφαρμογής και αξιοποίησης τεχνολογιών και μεθοδολογιών προάσπισης της ιδιωτικότητας σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης, καθώς και η διαμόρφωση ενός πλαισίου για την ολοκληρωμένη διαχείριση των ψηφια-

κών ταυτοτήτων για όλες τις συμμετέχουσες οντότητες. Η εγκαθίδρυση και διατήρηση σχέσεων εμπιστοσύνης αφορά όλες τις εμπλεκόμενες οντότητες και άπτεται θεμάτων, όπως η ασφάλεια των συναλλαγών, η προστασία προσωπικών δεδομένων, η διαφάνεια των διαδικασιών και η σωστή ενημέρωση των πολιτών (Κουντζέρης, 2011).

Αρχικά μελετήθηκαν και αποτυπώθηκαν οι σημαντικότερες προσεγγίσεις σε παγκόσμιο επίπεδο, αναφορικά με το συνολικό στρατηγικό σχεδιασμό για την ανάπτυξη και προώθηση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, τα πλαίσια διαλετουργικότητας και Ψηφιακής Αυθεντικοποίησης. Εν συνεχεία αποτυπώθηκαν οι απαιτήσεις ασφάλειας και ιδιωτικότητας σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης, σε επίπεδο τελικών χρηστών, παρόχων των ηλεκτρονικών υπηρεσιών, καθώς και του ισχύοντος νομικού και κανονιστικού πλαισίου. Επιπρόσθετα, αναγνωρίστηκαν και καταγράφηκαν συγκεντρωτικά τόσο οι δυνητικές απειλές και όσο και οι πιθανές επιπτώσεις τους σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης, αναφορικά με την απώλεια των προηγούμενων απαιτήσεων, και προτάθηκαν τρόποι αντιμετώπισης και ελαχιστοποίησής τους. Δεδομένης της ιδιαίτερης σημασίας συσχέτισης - αντιστοίχισης της πραγματικής ταυτότητας του τελικού χρήστη με συγκεκριμένη ψηφιακή ταυτότητα και της διαχείρισής της, καθ' όλη τη διάρκεια του κύκλου ζωής της, εξετάστηκαν οι διαφορετικές πρακτικές-μεθοδολογίες ταυτοποίησης και διασύνδεσης μερικών ψηφιακών ταυτοτήτων σε ψηφιακά πιστοποιητικά X.509 v3 και προτάθηκαν ολοκληρωμένες μεθοδολογίες ενσωμάτωσης και διαχείρισης τομεακών αναγνωριστικών, σε περιβάλλοντα ομόσπονδων ταυτοτήτων και σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης 2.0. Προς την κατεύθυνση της εγκαθίδρυσης και διατήρησης των προαναφερθεισών σχέσεων εμπιστοσύνης, μελετήθηκε και προτάθηκε ένα ολοκληρωμένο Πλαίσιο Ψηφιακής Αυθεντικοποίησης, μέσω του προσδιορισμού των αντίστοιχων επιπέδων εμπιστοσύνης, αυθεντικοποίησης και εγγραφής των τελικών χρηστών. Κατά το σχεδιασμό λήφθηκαν υπόψη οι απαιτήσεις και οι περιορισμοί του ελληνικού νομικού και κανονιστικού πλαισίου, προκειμένου αυτό να μπορεί να εφαρμοστεί στην Ελληνική Δημόσια Διοίκηση. Τέλος, μελετήθηκε η αξιοποίηση των Πολιτικών και των Προτιμήσεων Ιδιωτικότητας και προτάθηκε για πρώτη φορά μία ολοκληρωμένη αρχιτεκτονικής ενσωμάτωσης και αξιοποίησής τους σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης. Στόχος της συγκεκριμένης αρχιτεκτονικής είναι να απλουστεύσει την παροχή ηλεκτρονικών υπηρεσιών, να παρέχει στους τελικούς χρήστες τον απαραίτητο έλεγχο για τη συλλογή, επεξεργασία και αποθήκευση των προσωπικών τους δεδομένων καθώς και τη διαβεβαίωση για την τήρηση των αντίστοιχων νομικών και κανονιστικών απαιτήσεων από την πλευρά των παρόχων.

7.2 Κατευθύνσεις Μελλοντικής Έρευνας

Η μελλοντική έρευνα επικεντρώνεται σε δύο βασικούς άξονες. Ο πρώτος αφορά στην αξιοποίηση της αρχιτεκτονικής που προτείνεται για πρώτη φορά στο Κεφάλαιο 6 και την περαιτέρω ανάπτυξή της με την εισαγωγή ενός σημασιολογικού πλαισίου που θα βασίζεται σε μία οντολογία (*ontology*). Το συγκεκριμένο πλαίσιο θα μοντελοποιεί τις θεμελιώδεις αρχές και απαιτήσεις, όπως αυτές προσδιορίζονται από το ισχύον νομικό και κανονιστικό πλαίσιο. Η οντολογία θα αποτελεί το φορμαλιστικό (*Formal*) ορισμό των κανόνων ιδιωτικότητας καθώς και των πολιτικών και των προτιμήσεων ιδιωτικότητας των παρόχων και των χρηστών αντίστοιχα, με σκοπό την δημιουργία ενός ολοκληρωμένου μηχανισμού λήψης αποφάσεων, αναφορικά με τη συλλογή, επεξεργασία και περαιτέρω μετάδοση των προσωπικών δεδομένων που αξιοποιούνται σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης. Η προτεινόμενη αρχιτεκτονική παρουσιάζεται παρακάτω στο Σχήμα 7-1 και αποτελεί επέκταση των προσεγγίσεων που έχουν προταθεί σε Έξυπνα Περιβάλλοντα και σε Π.Σ. Διαδικτυακής Τηλεφωνίας (*VoIP*), (Τσούμας, 2007), (Λιουδάκης, 2008) καθώς και σε Π.Σ. Ανίχνευσης Εισβολών (Kostopoulos et al., 2013).



Σχήμα 7-1: Προτεινόμενη Αρχιτεκτονική Πράκτορα Διαχείρισης Ιδιωτικότητας

Ο δεύτερος άξονας αφορά στη μελέτη και ενσωμάτωση, στο προτεινόμενο πλαίσιο, επικαιροποιημένων νομικών και κανονιστικών διατάξεων, σε Εθνικό και Ευρωπαϊκό επίπεδο. Πρόσφατο παράδειγμα αποτελεί ο κανονισμός 611/2013 της Ε.Ε. σχετικά με "*Τα εφαρμοστέα μέτρα για την*

κοινοποίηση παραβιάσεων προσωπικών δεδομένων βάσει της Οδηγίας 2002/58/ΕΚ". Παρόλο που ο συγκεκριμένος κανονισμός αφορά παρόχους ηλεκτρονικών επικοινωνιών, η Δημόσια Διοίκηση οφείλει να αποτελεί πρότυπο για όλους τους παρόχους υπηρεσιών και να διασφαλίζει τη διατήρηση του κλίματος εμπιστοσύνης, ακόμα και μέσω της κοινοποίησης παραβιάσεων προσωπικών δεδομένων. Σύμφωνα με πρόσφατη μελέτη της Rapid7 (Parid7, 2012), στο διάστημα μεταξύ 1ης Ιανουαρίου 2009 και 31ης Μαΐου 2012 αναγνωρίστηκαν συνολικά 268 περιστατικά παραβιάσεων προσωπικών δεδομένων και μη εξουσιοδοτημένης κοινοποίησης προσωπικών αναγνωριστικών σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης των Η.Π.Α.

ΣΥΝΤΟΜΕΥΣΕΙΣ ΚΑΙ ΑΚΡΩΝΥΜΙΑ

Όρος - Ακρωνύμιο	Επεξήγηση
Back-End	Οπίσθιο Τμήμα Ηλεκτρονικής Υπηρεσίας
eGIF	e-Government Interoperability Framework
eIDM	Electronic Identity Management
FIM	Federated Identity Management
Front-End	Εμπρόσθιο Τμήμα Ηλεκτρονικής Υπηρεσίας
GSIS	General Secretary of Information Systems
IdN	National Identity Card Number
IT	Information Technology
PET	Privacy Enhancing Technologies
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SIItype	Sensitive Identification Information type
SQL	Structured Query Language
SSL	Secure Socket Layer
URL	Uniform Resource Locator
XML	Extensible Markup Language
ΑΔ	Αριθμός Διαβατηρίου
ΑΔΔ	Αρχή Διαχείρισης Δεδομένων
ΑΔΤ	Αριθμός Δελτίου Ταυτότητας
ΑΔΤ	Αριθμός Δελτίου Ταυτότητας
ΑΜΚΑ	Αριθμός Μητρώου Κοινωνικής Ασφάλισης
ΑΦΕ	Αποδεικτικού Φορολογικής Ενημερότητας
ΔΔ	Δημόσια Διοίκηση
ΔΟΥ	Δημόσια Οικονομική Υπηρεσία

Όρος - Ακρωνύμιο	Επεξήγηση
ΗΔ	Ηλεκτρονική Διακυβέρνηση
ΚΔΠ	Κεντρική Διαδικτυακή Πύλη
Λ.Σ.	Λειτουργικό Σύστημα
Π.Σ.	Πληροφοριακό Σύστημα
ΠΔ	Προεδρικό Διάταγμα
ΠΔΙ	Πράκτορας Διαχείρισης Ιδιωτικότητας
ΠΨΑ	Πλαίσιο Ψηφιακής Αυθεντικοποίησης
ΤΠΕ	Τεχνολογίες Πληροφοριών και Επικοινωνιών
ΤΠΕ	Τεχνολογίες Πληροφοριών και Επικοινωνιών
ΥΔΚ	Υποδομή Δημοσίου Κλειδιού
ΦΕΚ	Φύλλο Εφημερίδας της Κυβερνήσεως
ΦΠΑ	Φόρος Προστιθέμενης Αξίας

ΒΙΒΛΙΟΓΡΑΦΙΑ

Anderson, A., 2006. A comparison of two privacy policy languages: EPAL and XACML. Alexandria, 2006. ACM.

Auerbach, N., 2004. *Anonymous Digital Identity in e-Government*. Zurich: University of Zurich.

Baldoni, R., 2012. Federated Identity Management systems in e-government: the case of Italy. *Electronic Government, an International Journal*, 9(1), pp.64 - 84.

Baldwin, A., Casassa Mont, M., Beres, Y. & Shiu, S., 2008. *Assurance for Federated Identity Management*. Bristol: HP Laboratories.

Barker, K. et al., 2009. A Data Privacy Taxonomy. London, 2009. Springer-Verlag.

Barth, M. & Mitchell, J., 2005. Enterprise privacy promises and enforcement. Long Beach, 2005. ACM.

Bertino, E., Carminati, B. & Ferrari, E., 2002. A Temporal Key Management Scheme for Secure Broadcasting of XML Documents. Berlin, 2002. ACM.

Bertino, E. et al., 2004. Selective and Authentic Third-Party Distribution of XML D0cuments. *Transactions on Knowledge and Data Engineering*, 16(10), pp.1263 - 1278.

Books LLC , 2010. *Password Cracking Software: Password Cracking, Dsniff, John the Ripper, Cain and Abel, Saminside, L0phtcrack, Ophcrack, Lastbit, Rainbowcrack*. 1st ed. New York: Books LLC.

Borins, S., 2010. Strategic Planning from Robert McNamara to Gov 2.0. *Public Administration Review*, 70(S1), pp.220 - 221.

Brandeis, P. & Warre, S., 1980. *The Right to Privacy*. Cambridge: Harvard Law Review.

Buecker, A., Ashley, P. & Readshaw, N., 2008. *Federated Identity and Trust Management*. New York: IBM Red Books.

Buell, D.A. & Sandhu, R., 2003. Identity management. *Internet Computing, IEEE*, 7(6), pp.26 - 28.

Burr, W. et al., 2011. *Electronic Authentication Guidelines - Special Publication 800-63-1*. Gaithersburg: NIST.

Camp, L., 2004. Digital Identity. *Technology and Society, IEEE*, 23(3), pp.34 - 41.

Cannon, J., 2004. *Privacy: What Developers and IT Professionals Should Know*. 1st ed. London: Addison-Wesley.

Carminati, B. & Ferrari, E., 2005. Trusted Privacy Manager: A System for Privacy Enforcement. Tokyo, 2005. IEEE.

CERI, 2003. *Rechtliche Rahmenbedingungen für E-Government*. Hamburg: Hans-Bredow Institut.

Chow, R. et al., 2009. ontrolling data in the cloud: outsourcing computation without outsourcing control. Chicago , 2009. ACM.

Clarke, R., 1997. *Introduction to Dataveillance and Information Privacy, and Definitions and Terms*. Australia: Xamax Consultancy Pty Ltd.

Clauß, S. & Köhntopp, M., 2001. Identity management and its support of multilateral security. *Computer Networks, Elsevier*, 37(2), pp.205 – 219.

Corradini, F., Paganelli, E. & Polzonetti, A., 2007. The e-Government digital credentials. *Int. J. of Electronic Governance, Inderscience*, 1(1), pp.17 - 37.

Coursey, D. & Norris, D., 2008. Models of E-Government: Are They Correct? An Empirical Assessment. *Public Administration Review*, 68(3), pp.523 – 536.

Danziger, J. & Andersen, K., 2002. The Impacts of Information Technology on Public Administration: An Analysis of Empirical Research from the "Gloden Age" of Transformation. *International Journal of Public Administration*, 25(5), pp.591 - 627.

de Kool, D. & van Wamelen, J., 2008. Web 2.0: A New Basis for E-Government?. Damascus, 2008. IEEE.

Dutton, W., Guerra, G., Zizzo, D. & Peltu, M., 2005. The cyber trust tension in E-government: Balancing identity, privacy, security. *Information Polity - Public Administration in the Information Society: Essays in Risk and Trust*, 10(1,2), pp.13 - 23.

EC, 2010. *Towards interoperability for European Public Service*. Brussels: European Commision.

Efraimidis, P., Drosatos, G., Nalbadis, F. & Tasidou, A., 2008. Towards Privacy in Personal Data Management. Samos, 2008. IEEE.

e-GIF, 2009. *Greek e-Government Interoperability Framework*. [Online] Available at: http://www.e-gif.gov.gr/ [Accessed 6 April 2013].

ENISA, 2009. *Cloud Computing Security Risk Assessment*. Herakleion: European Network and Information Security Agency.

ENISA, 2010. *Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments*. Heraklion: European Network and Information Security Agency.

Evangelidis, A., 2004. FRAMES – A Risk Assessment Framework for e-Services. *Electronic Journal of e-Government*, 2(1), pp.21 - 30.

Ferguson, N. & Schneier, B., 2003. *Practical Cryptography*. 1st ed. London: Wiley.

Ferguson, N. & Schneier, B., 2003. *Practical Cryptography*. 1st ed. New York: John Wiley & Sons.

Fischer-Hübner, S., 2001. Design and Use of Privacy-Enhancing Security Mechanisms. In K. Brunnstein, ed. *IT-Security and Privacy*. 1st ed. Hamburg: Springer LNCS. pp.107 - 166.

Gapgemini, 2007. *The User Challenge Benchmarking the Supply of Online Public Services*. Brussles: Directorate General for Information Society and Media.

Geneiatakis, D., Lambrinoudakis, C. & Gritzalis, S., 2009. A Hierarchical Model for Cross-Domain Communication of Health Care Units. Australia, 2009. IEEE Explore.

Gotoh, R., 2008. Assessing Performance of e-Government Services for Business Users. Melbourne, 2008. Academic Conferences.

Gouscos, D., Georgiadis, P. & Sagris, T., 2000. From Introvert IT Systems to Extrovert eServices, e-Government as an Enabler for e-Citizens and e-Business - A frameowrk of Principles. Madrid, 2000. Proceedings of the Electronic Business and Electronic Work 2000 Conference (EBEW 2000), IOS Press.

Gritzalis, S. & Lambrinoudakis, C., 2002. Security Requirements of e-Government Services: An Organizational Framework. Las Vegas, 2002. CSREA Press.

Grönlund, Å. & Horan, T., 2005. Introducing e-Gov: History, Definitions, and Issues. *Communications of the Association for Information Systems*, 15(1), pp.713 - 729.

Hahamis, P., J., I. & Healy, M., 2005. e-Government in Greece: Bridging the Gap between Need and Reality. *Electronic Journal of e-Government*, 3(4), pp.185 - 192.

Hayat, A., Leitold, H., Rechberger, C. & Rossler, T., 2004. *Survey on EU's Electronic-ID Solutions*. Vienna: Austria Secure Information Technology Center.

Henderson, M., Coulter, R., Dawson, E. & Okamoto, E., 2002. Modelling Trust Structures for Public Key Infrastructures. Sidney, 2002. Springer LNCS.

Hoegg, R., Martignoni, R., Meckel, M. & Stanoevska, K., 2006. Overview of business models for Web 2.0 communities. Dresden, 2006. GeNeMe conference proceedings.

Hong, Y., Lu, S., Liu, Q. & Wang, L., 2007. A Hierarchical Approach to the Specification of Privacy Preferences. Dubai, 2007. IEEE.

ISO/IEC 27001, 2013. *Information technology - Security Techniques - Information Security Management Systems - Requirements*. -: ISO - International Organization for Standardization.

Jøsang, A. & Pope, S., 2005. User Centric Identity Management. Sidney, 2005. AusCERT Conference Proceedings.

Jun, S., Zhenfu, C. & Rongxing, L., 2006. An improved deniable authentication protocol. *Networks*, 48(4), pp.179 – 181.

Kostopoulos, D. et al., 2013. Real Time Threat Prediction, Identification and Mitigation for Critical Infrastructure Protection using Semantics, Event Processing and Sequential Analysis. Amsterdam, 2013. Springer LNCS.

Kujawski, M., 2013. *Government 2.0 - Best Practices Wiki*. [Online] Available at: http://government20bestpractices.pbworks.com/ [Accessed 8 Augustus 2013].

Kumaraguru, P., Cranor, L., Lobo, J. & Calo, S., 2007. A Survey of Privacy Policy Languages. Pittsburgh, 2007. Workshop on Usable IT Security Management (USM '07).

Lambrinoudakis, C., Gritzalis, S., Dridi, F. & Pernul, G., 2003. Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. *Securing Computer Communications with Public Key Infrastructure*, 26(16), pp.1873 – 1883.

Layton, T..P.., 2006. *Information Security: Design, Implementation, Measurement and Compliance*. 1st ed. New York: Auerbach Publications.

Liberty Alliance, 2006. *Liberty ID-FF Architecture Overview*. New Jersey: Liberty Alliance Project.

Liberty Alliance, 2006. *Liberty ID-WSF Web Services Framework Overview*. New Jersey: Liberty Alliance Project.

Liberty Alliance, 2007. *Liberty IGF Privacy Constraints Specification*. New Jersey: Libert Alliance Project.

Madsen, P., Mont, C..M. & R., W., 2006. *A Privacy Polocy Framework - A position paper for the W3C Workshop of Privacy Policy Negotiation*. -: W3.

Markellos, K., Markellou, P., Panayiotaki, A. & Stergianeli, E., 2007. Current State of Greek E-Government Initiatives. *Journal of Business Systems, Governance and Ethics*, 2(3), pp.67 - 88.

Massey, A. & Antón, A., 2008. A Requirements-based Comparison of Privacy Taxonomies. Washington, 2008. IEEE CPS.

McRobb, S. & Stahl, B., 2007. Privacy as a shared feature of the e-phenomenon: a comparison of privacy policies in e-government, e-commerce and e-teaching. *International Journal of Information Technology and Management*, 6(2 - 4), pp.232 - 249.

Meijer, A. et al., 2012. Government 2.0: Key Challenges to Its Realization. *Electronic Journal of e-Government*, 10(1), pp.59 - 69.

Meta, 2005. *Privacy Enhancing Technologies*. Copenhagen: Ministry of Science, Technology and Innovation.

Muir, A. & Oppenheim, C., 2002. National Information Policy Developments Worldwide in Electronic Government. *Journal of Information Science*, 28(3), pp.173 - 186.

Ndou, V., 2004. E-government for developing countries: opportunities and challenges. *The Electronic Journal on Information Systems in Developing Countries* , 18(1), pp.1 - 24.

NIST, 1985. *Password Usage*. Gaithersburg: National Institute of Standards and Technology.

NIST, 2002. *Security Requirements for Cryptographic Modules*. Gaithersburg: National Institute of Standards and Technology.

NIST, 2011. *Guidelines on Security and Privacy in Public Cloud Computing*. Gaithersburg: National Insitute of Standards and Technology.

NIST, 2011. *The NIST Definition of CLoud Computing*. Gaithersburg: National Institute of Standards and Technology.

NIST, 2012. *Secure Hash Standard (SHS)*. Gaithersburg: National Institute of Standards and Technology.

NZ eGov, 2009. *Online Authentication Threats and Attacks | ICT.govt.nz*. [Online] Available at: http://ict.govt.nz/guidance-and-resources/standards-compliance/authentication-standards/authentication-key-strengths-standard/5-online-authenticati/ [Accessed 27 March 2013].

OASIS, 2006. *Web Services Policy Framework*. Burlington: OASIS.

OASIS, 2007. *WS - Trust Specifications v.1.3.* Burlington: OASIS.

OECD, 1980. *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data*. [Online] Available at: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [Accessed 14 May 2013].

Osimo, D., 2008. *Web 2.0 in Government: Why and How?* Brussels: European Comission Insitute for Prospective Technological Studies.

Ostergaard, S. & Hvass, M., 2008. *eGovernment 2.0 – How can Government benefi t from web 2.0?* Copenhagen: IBM Demark.

Parid7, 2012. *Data Breaches in the Government Sector*. Boston: Parid7.

Park, J. et al., 2006. *Internet X.509 Public Key Infrastructure Subject Identification Method (SIM) - RFC 4683*. -: RFC.

Pato, J., 2003. *Identity Management: Setting the Context*. Cambridge: HP Laboratories.

Pfitzmann, B. & Waidner, M., 2003. Federated identity-management protocols. Cambridge, 2003. Springer - Verlag.

PICOS, 2008. *D2.1 Taxonomy*. Leuven: PICOS Project - Privacy and Identity Management for Community Services.

Ramaraj, P. & Mukerji, B., 2012. Security and Privacy Issues in E-Government. In M. Shareef, N. Archer & S. Dutta, eds. *E-Government Service Maturity and Development: Cultural, Organizational and Technological Perspectives*. New York: IGI Global. pp.236 - 248.

Rezgui, A., Wen, Z. & Bouguettaya, A.., 2002. Enforcing privacy in interoperable e-government applications. Los Angeles, 2002. ACM.

Rosenberg, R., 1992. *The Social Impact of Computers*. San Diego: Academic Press.

Rössler, T.., 2010. *E-Government und Cloud-Computing*. Graz: EGIZ e-Government Innovationszentrum.

Satizábal, C., Forne, J., Hernández-Serrano, S. & Pegueroles, J., 2006. Building Hierarchical Public Key Infrastructures in Mobile Ad-Hoc Networks. Hong Kong, 2006. Springer LNCS.

Schneier, B., 2005. *Cryptanalysis of SHA-1*. London: Bruce Schneier Blog.

Schneier, B., Goodrich, M. & Tamassia, R., 2006. *Introduction to Security and Applied Cryptography*. 1st ed. London: John Wiley & Sons.

Sedek, A., Sulaiman, S. & Omar, A., 2011. A systematic literature review of interoperable architecture for e-Government Portals. Malaysia, 2011. IEEE.

Šilić, M., Krolo, J. & Delac, J., 2010. Security Vulnerabilities in Modern Web Browser Architecture. Opatija, 2010. IEEE.

Solis, B. & Thomas, J., 2013. *The Conversation Prism*. [Online] Available at: http://www.theconversationprism.com/ [Accessed 22 June 2013].

Solove, D., 2009. *A Taxonomy of Privacy*. Washington: University of Pennsylvania.

Stefanova, K., Kabakchieva, D. & Nikolov, R., 2010. Design Principles of Identity Management Architecture Development for Cross-Border eGovernment Services. *Electronic Journal of e-Government*, 8(2), pp.189 - 202.

Tambouris, E. & Wimmer, M., 2005. Online One-Stop Government: A Signle Point of Access to Public Services. In W. Huang, K. Siau & K. Wei, eds. *Electronic Government - Strategies and Implementation*. Athens: Idea Group Publishing. pp.115 - 144.

Tapscott, D., Williams, A. & Herman, D., 2008. *Government 2.0: Transforming government and governance for the twenty-first century*. Sunnyvale: nGenera Insight.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C. & Gritzalis, S., 2010. Unifying ISO Security Standards Practices into a Single Security Framework. Port Elisabeth, 2010. Springer LNCS.

United Nations, 2003. *Guiding Principles for Successful e-Government*. New York: UN.

United Nations, 2005. *E-government Readiness Report - From E-government to E-inclusion*. New York: UN.

United Nations, 2010. *E-Government 2010 Survey Leveraging e-government at a time of financial and economic crisis*. New York: UN.

United Nations, 2012. *E-Government Survey 2012 E-Government for the People*. New York: UN.

United Nations, 2013. *E-Government Development Database: Global Reports*. [Online] Available at: http://unpan3.un.org/egovkb/global_reports/index.htm [Accessed 22 March 2013].

Vivo, M., Vivo, G. & Isern, G., 1998. Internet security attacks at the basic levels. *ACM SIGOPS Operating Systems Review*, 32(2), pp.4-15.

Votis, K., Alexakos, C., Vassiliadis, B. & Likothanassis, S., 2008. An Ontologically Principled Serivce-Oriented Architecture for Managing Distributed e-GOvernment Nodes. *Journal of Network and Computer Applications*, 31(2), pp.131 - 148.

Vrakas, N., Kalloniatis, C., Tsohou, A. & Lambrinoudakis, C., 2010. Privacy Requirements Engineering for Trustworthy e-Government Services. Berlin, 2010. Springer LNCS.

Wang, Y. & Kobsa, A., 2008. *Handbook of Research on Social and Organizational Liabilities in Information Systems*. 1st ed. New York: IGI Global.

Westin, A.., 1967. *Privacy and Freedom*. 1st ed. London: The Bodley Head.

Wyld, D. & Maurin, R., 2009. *Moving to the Cloud: An introduction to CLoud Computing in Government*. Louisiana: e-Government Series, Southeastern Louisina University.

Yee, O., 2007. A privacy controller approach for privacy protection in web services. 2007, 2007. Berlin.

Zhang, W. & Wang, Y., 2008. Towards building a semantic grid for e-Government applications. *WSEAS Transactions on Computer Research Journal*, 3(4), pp.273 - 282.

Zhao, M. & Smith, S., 2006. Modeling and Evaluation of Certification Path Discovery in the Emerging Global PKI. Turin, 2006. Springer LNCS.

Ακριβοπούλου, Χ., 2009. *Μεταξύ αυτονομίας και οικειότητας: αναπροσδιορίζοντας το δικαίωμα στην ιδιωτική ζωή*. Θεσσαλονίκη: Τμήμα Νομικής, ΑΠΘ.

Βέργη, Ε., 2009. *Η Διακυβέρνηση στην εποχή του Web 2.0*. Αθήνα: Παρατηρητήριο για την Κοινωνία της Πληροφορίας.

Γκρίτζαλης, Δ., 2004. *Ασφάλεια Πληροφοριακών Συστημάτων σε Περιβάλλοντα Υψηλής Ευπάθειας*. Σάμος: Πανεπιστήμιο Αιγαίου.

Γκρίτζαλης, Σ., Κάτσικας, Σ. & Γκρίτζαλης, Δ., 2003. *Ασφάλεις Δικτύων Υπολογιστών*. 2003rd ed. Αθήνα: Παπασωτηρίου.

Διακονικολάου, Κ. & Μυλωνόπουλος, Ν., 2004. *Το παρόν και το μέλλον των Ηλεκτρονικών Υπηρεσιών του Κράτους προς τις Επιχειρήσεις (Government to Business) στην Ελλάδα*. Αθήνα: Κοινωνία της Πληροφορίας.

Επιτροπή Συντονισμού της Ηλεκτρονικής Διακυβέρνησης, 2013. *Σχέδιο Κειμένου Βασικών Αρχών και Κατευθύνσεων: Εθνική Στρατηγική για την Ηλεκτρονική Διακυβέρνηση*. Αθήνα: Επιτροπή Συντονισμού της Ηλεκτρονικής Διακυβέρνησης.

Ιγγλεζάκης, Ι., 2007. *Εισαγωγή στο δίκαιο της πληροφορικής*. 1st ed. Αθήνα: Σάκκουλα.

Καλλονιάτης, Χ., 2011. *Ασφάλεια Δεδομένων στην Κοινωνία της Πληροφορίας - Ιδιωτικότητα*. Μυτιλήνη: Πανεπιστήμιο Αιγαίου.

Καμπουράκης, Γ., ΓΚρίτζαλης, Σ. & Κάτσικας, Σ., 2006. *Ασφάλεια Ασυρμάτων και Κινητών Δικτύων Επικοινωνιών*. 1st ed. Αθήνα : Παπασωτηρίου.

Κιοσσέ, Ε., 2011. *Η πορεία της Ηλεκτρονικής Διακυβέρνησης στις χώρες της Ε.Ε. και την Ελλάδα - Οι επιδόσεις των χωρών*. Θεσσαλονίκη: Πανεπιστήμιο Μακεδονίας.

Κουντζέρης, Α., 2010. *Ηλεκτρονική ταυτότητα πολιτών και επιλογές πολιτικής & υποδομών – η Ευρωπαϊκή εμπειρία*. Αθήνα: Παρατηρητήριο για την Κοινωνία της Πληροφορίας.

Κουντζέρης, Α., 2011. *Διερεύνση της αντίληψης των Ελλήνων πολιτών σχετικά με τη χρήση ηλεκτρονικών υπηρεσιών που απαιτούν ταυτοποίηση*. ΑΘήνα: Παρατηρητήριο για την Κοινωνία της Πληροφορίας.

ΚτΠ, 2008. *Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Πρότυπα Διαλειτουργικότητας*. Αθήνα: Κοινωνία της Πληροφορίας.

ΚΤΠ, 2008. *Πλαίσιο Διαλειτουργικότητας και Υπηρεσιών Ηλεκτρονικών Συναλλαγών*. Αθήνα: Κοινωνία της Πληροφορίας Α.Ε.

ΚτΠ, 2009. *Δ' Έκδοση Πλαισίου Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, Τεύχος Γ, Πλαίσιο Ψηφιακής Αυθεντικοποίησης*. Αθήνα: Κοινωνία της Πληροφορίας Α.Ε.

Λαζαρίδης, Σ., 2011. *Ανάλυση Πολιτικών και Πρακτικών Εθνικής Ηλεκτρονικής Ταυτότητας (eID) στην Ευρώπη*. Σάμος: Πανεπιστήμιο Αιγαίου.

Λαμπρινουδάκης, Κ., Γκρίτζαλης, Σ., Μήτρου, Λ. & Κάτσικας, Σ., 2010. *Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών*. 1st ed. Αθήνα: Παπασωτηρίου.

Λιουδάκης, Γ., 2008. *Προστασία Προσωπικών Δεδομένων σε Έξυπνα Περιβάλλοντα*. Αθήνα: Εθνικό Μετσόβιο Πολυτεχνείο.

Λιουδάκης, Γ., 2008. *Προστασία Προσωπικών Δεδομένων σε Έξυπνα Περιβάλλοντα*. Αθήνα: Εθνικό Μετσόβιο Πολυτεχνείο.

Μήτρου, Λ., 2002. *Το δίκαιο στην κοινωνία της πληροφορίας*. 1st ed. Αθήνα: Σάκκουλα.

Μήτρου, Λ., 2006. *Προστασία Προσωπικών Δεδομένων*. Σάμος: Πανεπιστήμιο Αιγαίου.

Μήτρου, Λ., 2010. Η Προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες. Η νομική διάσταση. In Κ. Λαμπρινουδάκης, ed. *Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών*. Αθήνα: Παπασωτηρίου. pp.505 - 552.

Παρατηρητήριο για τη Διοικητική Μεταρρύθμιση, 2013. *Εξέλιξη των 20 βασικών υπηρεσιών Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα*. Αθήνα: ΚΤΠ Α.Ε.

Πουλούδη, Α., Πουλυμενάκου, Α., Πρασοπούλου, Ε. & Καλλιαμβάκου, Ε., 2007. *Διαχείριση Ταυτότητας στις Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης*. Αθήνα: ebusiness forum.

Τσούμας, Β., 2007. *Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων με Οντολογίες*. Αθήνα: Οικονομικό Πανεπιστήμιο Αθηνών.

ΠΑΡΑΡΤΗΜΑ Ι - ΕΡΕΥΝΗΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ

Οι επιστημονικές δημοσιεύσεις που παρουσιάζονται παρακάτω περιλαμβάνουν εργασίες που έχουν δημοσιευθεί σε διεθνή επιστημονικά περιοδικά και συνέδρια ύστερα από διαδικασίες πλήρους κρίσης και σχετίζονται με την έρευνα που διεξήχθη στο πλαίσιο της παρούσας διατριβής[5].

Σε Διεθνή Επιστημονικά Περιοδικά μετά από Πλήρη Κρίση

J1 P. Drogkaris, S. Gritzalis, C. Lambrinoudakis, "*Employing Privacy Policies and Preferences in Modern e-Government Environments*", Special Issue on "Security and Privacy of E-Government Applications and Services" of the International Journal of Electronic Governance, 2013, Inderscience Publishers ***(0)***

J2 P. Drogkaris, S. Gritzalis, C. Lambrinoudakis, "*A Hierarchical Multitier Approach for Privacy Policies in e-Government Environments*", the International Journal of Electronic Governance, (Under Review) , Inderscience Publishers ***(0)***

Σε Διεθνή Επιστημονικά Συνέδρια μετά από Πλήρη Κρίση

C1 D. Núñez, I. Agudo, P. Drogkaris, S. Gritzalis, "Identity Management Challenges for Intercloud Applications", 1st International Workshop on Security & Trust for Applications in Virtualised Environments (STAVE 2011), C. Skianis, (Ed.), pp. 198 - 204, June, 2011, Loutraki, Greece, Communications in Computer and Information Science Series CCIS, Springer ***(4)***

C2 P. Drogkaris, S. Gritzalis, "*Attaching Multiple Personal Identifiers in X.509 Digital Certificates*", EuroPKI 2010 7th European Workshop on Public Key Services, Applications and Infrastructures, J. Camenisch and C. Lambrinoudakis, (Eds.), pp. 171-177, September 2010, Athens, Greece, Lecture Notes in Computer Science LNCS, Springer ***(0)***

C3 P. Drogkaris, S. Gritzalis, C. Lambrinoudakis, "*Transforming the Greek e-Government Environment towards the e-Gov 2.0 Era*", EGOVIS'10 International Conference on ***(5)***

[5] Ο αριθμός στην παρένθεση υποδηλώνει τον αριθμό των ετεροαναφορών ανά δημοσίευση από μη συνεργάτες

Electronic Government and the Information Systems Perspective, K. Andersen, E. Francesconi, A. Gronlund, T. M. Engers. (Eds.), pp. 142 -149, September 2010, Bilbao, Spain, Lecture Notes in Computer Science LNCS, Springer

C4 P. Drogkaris, C. Lambrinoudakis, S. Gritzalis, "*Introducing Federated Identities to One-Stop-Shop e-Government Environments: The Greek Case*", eChallenges 2009 19th Conference, P. Cunningham, M. Cunningham (Eds.), pp. 115 – 121, October 2009, Istanbul, Turkey, eChallenges e-2009 Conference Proceedings ***(0)***

C5 P. Drogkaris, S. Gritzalis, C. Lambrinoudakis, "*Enabling Secure Data Management in e-Government Environments: The Greek Case*", EGOV'09 8th International Conference on Electronic Government, EGOV 2009, H. J. Scholl, M. Janssen, R. Traunmüller, M. A. Wimmer (Eds.), pp. 138-145, September 2009, Linz, Austria, Trauner Verlag Schriftenreihe Informatik ***(0)***

C6 P. Drogkaris, D. Geneiatakis, S. Gritzalis, C. Lambrinoudakis, L. Mitrou, "Towards an Enhanced Authentication Framework for eGovernment Services: The Greek Case", EGOV'08 7th International Conference on Electronic Government, E. Ferro, J. Scholl, M. Wimmer (Eds.), pp. 189-196, September 2008, Torino, Italy, Trauner Verlag Schriftenreihe Informatik ***(6)***

Παραδοτέα Χρηματοδοτούμενων Ερευνητικών - Μελετητικών Έργων

D1 Παραδοτέο ΠΑ1.7: Δ' Έκδοση Πλαισίου Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, Τεύχος Γ, Πλαίσιο Ψηφιακής Αυθεντικοποίησης. 2009, Κοινωνία της Πληροφορίας ΑΕ - Υπουργείο Εσωτερικών Δημόσιας Διοίκησης και Αποκέντρωσης - PLANET ΑΕ, ΕΠΙΣΕΥ/ΕΜΠ, ATC - Πανεπιστήμιο Αιγαίου **-**

Οι επιστημονικές δημοσιεύσεις που παρουσιάζονται παρακάτω περιλαμβάνουν εργασίες που έχουν δημοσιευθεί σε διεθνή επιστημονικά συνέδρια ύστερα από διαδικασίες πλήρους κρίσης και σχετίζονται με την έρευνα που διεξήχθη παράλληλα με την παρούσα διατριβή.

Σε Διεθνή Συνέδρια μετά από Πλήρη Κρίση

C7 D. Kostopoulos, V. Tsoulkas, P. Drogkaris, G. Leventakis, "*Risk Management and Data Monitoring of Critical Infrastructures Combining Event Analytics with Sequential Inspection*", 2nd International Conference on Vulnerability and Risk Analysis and Management (ICVRAM 2014), (to appear), July 2014, UK, ASCE ***(0)***

C8 D. Kostopoulos, V. Tsoulkas, G. Leventakis, P. Drogkaris, V. Politopoulou, "*Real Time Threat Prediction, Identification and Mitigation for Critical Infrastructure Protection using Semantics, Event Processing and Sequential Analysis*", 8th International Workshop on Critical Information Infrastructures Security (CRITIS 2013), September 2013, Holland, Springer LNCS ***(0)***

C9 D. Kostopoulos, V. Tsoulkas, G. Leventakis, P. Drogkaris, V. Politopoulou, "*A Blend of Semantic Monitoring and Intrusion Detection Systems for the Protection of Critical Infrastructures: Research efforts within the Greek Cybercrime Center*", Fifth International Conference on Computanional Intelligence, Communication Systems and Networks (CICSYN 2013), G. Romero, A. Orsoni, (eds), , June 2013, Spain, IEEE CPS ***(0)***

C10 D. Kostopoulos, V. Tsoulkas, G. Leventakis, P. Drogkaris, V. Politopoulou, "*Semantic Systems Modeling and Monitoring for Real Time Decision Making: Results and Next Steps within the Greek Cyber Security Center of Excellence*", AMSS 15th International Conference on Modelling and Simulation (UK-SIM 2013), April 2013, Cambridge UK, IEEE CPS ***(0)***

ΠΑΡΑΡΤΗΜΑ ΙΙ - ΣΥΝΤΟΜΟ ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ

Ο Προκόπιος Δρογκάρης γεννήθηκε στη Σπάρτη, Λακωνίας το 1982. Είναι διπλωματούχος Μηχανικός Πληροφοριακών και Επικοινωνιακών Συστημάτων της Σχολής Θετικών Επιστημών του Πανεπιστημίου Αιγαίου και κάτοχος μεταπτυχιακού τίτλου σπουδών (Msc) στα Πληροφοριακά Συστήματα της Σχολής Πληροφορικής του Πανεπιστημίου City του Λονδίνου.

Τα ερευνητικά του ενδιαφέροντα εντάσσονται στη γνωστική περιοχή της Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων και των Τεχνολογιών Προστασίας και Διαχείρισης της Ιδιωτικότητας σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης και Νεφοϋπολογιστικής. Είναι συγγραφέας 12 επιστημονικών δημοσιεύσεων σε επιστημονικά συνέδρια και περιοδικά ύστερα από διαδικασία κρίσης. Έχει αποτελέσει μέλος της επιτροπή προγράμματος 17 επιστημονικών συνεδρίων και εξωτερικός κριτής σε περισσότερα από 40. Έχει συμμετάσχει σε εθνικά ερευνητικά έργα και μελέτες της Κοινωνίας της Πληροφορίας, του Υπουργείου Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης και σε Ευρωπαϊκά ερευνητικά έργα του 7ου Προγράμματος Πλαισίου (*FP7*) και της Γενικής Διεύθυνσης DG HOME AFFAIRS της Ευρωπαϊκής Επιτροπής.

Από το 2010 έχει εργασθεί ως Εργαστηριακός Συνεργάτης στο τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών του Τ.Ε.Ι. Καλαμάτας καθώς και στα τμήματα Ηλεκτρονικών, Αυτοματισμού και Ηλεκτρονικών Υπολογιστικών Συστημάτων του Τ.Ε.Ι. Πειραιά. Το 2011 και το 2012 υπήρξε συντονιστής και εισηγητής του δημόσιου διαλόγου, σε Ευρωπαϊκό Επίπεδο, για την Εμπιστοσύνη και την Ασφάλεια, στο πλαίσιο του Ψηφιακού Θεματολογίου 2020 (*Digital Agenda 2020).* Τέλος, είναι μέλος του Τεχνικού Επιμελητηρίου Ελλάδας (Τ.Ε.Ε.) και της Ελληνικής Εταιρείας Επιστημόνων και Επαγγελματιών Πληροφορικής και Επικοινωνιών (Ε.Π.Υ.).